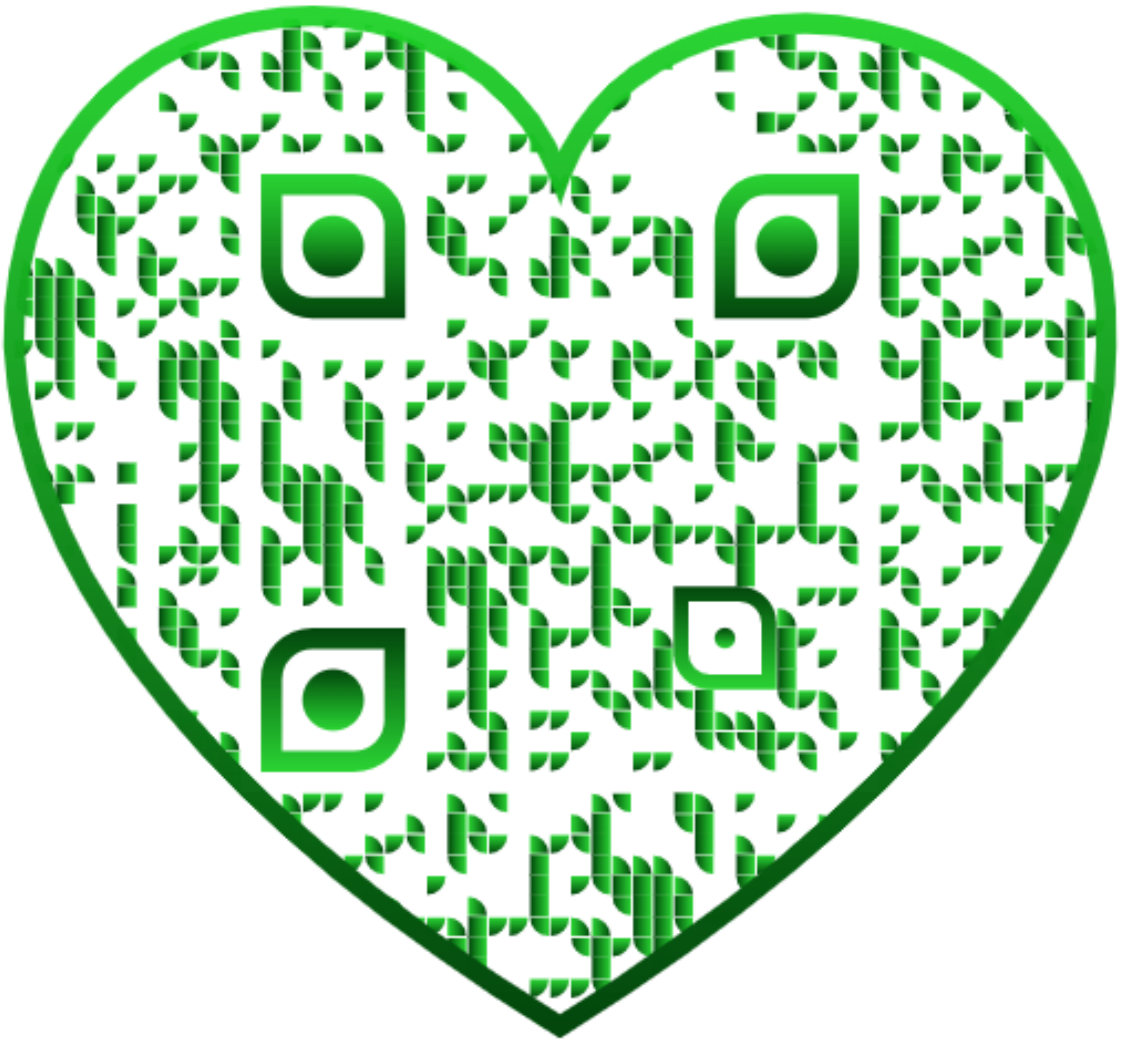
Tristan Nitot

surveillance://

Les libertés au défi du numérique :
comprendre et agir



Tristan Nitot

surveillance://

Les libertés au défi du numérique

Comprendre et agir

C&F éditions
2016

Table des matières

Couverture

Page de titre

Table des matières

Préface par Adrienne Charmet
Redonner du pouvoir d’agir face à la surveillance

Avant-propos

Première partie
Souriez, vous êtes surveillés !
Les dangers de la surveillance

1. Est-il si grave de perdre le contrôle de son ordinateur et de son smartphone ?
2. Les risques personnels
3. Google sait tout sur nous, voici comment
4. Facebook, la manipulation des masses et la démocratie
5. La surveillance des États
6. Big Data et grosses responsabilités
7. L’impact de la surveillance sur la société
8. Loi et vie privée
9. Mais, je n’ai rien à cacher !

Partie II
Au royaume d’internet, le code, c’est la loi
Les mécanismes de la surveillance

10. Contrôler pour ne pas être contrôlé
11. Que peut-on contrôler ?
12. Contrôle et informatique personnelle
13. Le code, c’est la loi
14. Internet change la donne
15. Le piège de la gratuité
16. Le modèle freemium
17. Faut-il avoir confiance en Apple ?
18. Smartphones et Cloud
19. Internet des objets, quantified self et beacons
20. Les services de renseignement

Partie III
Un autre réseau est possible
Inventer une approche de l’informatique en réseau limitant la surveillance

21. Sept principes pour reprendre le contrôle
22. Le logiciel libre
23. La maîtrise du serveur
24. Le recours au chiffrement
25. Penser le modèle d’affaire
26. Faire mieux que les systèmes centralisés

Partie IV
Un internaute averti en vaut dix
Limiter la surveillance au quotidien

27. Partir sur de bonnes bases
28. Choisir et personnaliser son navigateur
29. Côté messagerie
30. Paramétrer Google
31. Choisir son smartphone
32. Les médias sociaux
33. Le cloud

Et maintenant ?

Remerciements

Achevé d'imprimé

Préface

par Adrienne Charmet

Historienne de formation, Adrienne Charmet est née en 1979. Elle est, depuis avril 2014, coordinatrice des campagnes de la Quadrature du Net, association de défense des droits et libertés des citoyens dans l'espace numérique. Elle a auparavant dirigé les programmes de Wikimédia France, l'association qui soutient Wikipédia en France.

Redonner du pouvoir d'agir face à la surveillance

Écrire sur les données personnelles et leur protection, sur la vie privée à l'ère du numérique, c'est avancer au milieu de plusieurs écueils. L'écueil technique – comment expliquer en termes simples et compréhensibles par tous des pratiques et des mécanismes qui sont devenus tellement complexes qu'on a bien du mal, même en étant un utilisateur averti, à les comprendre. L'écueil de la paranoïa – comment continuer à utiliser quotidiennement les outils numériques lorsqu'on a pris conscience de la masse de données personnelles qui sont collectées, stockées, et qui circulent quotidiennement. L'écueil politique, qui nous laisse trop souvent amers devant les réponses dangereuses, inadaptées ou inexistantes des décideurs politiques face à un modèle qu'ils semblent ne pas comprendre. L'écueil de l'invisibilité, qui rend difficilement perceptible l'ampleur de la collecte de données et de la surveillance qui en découle, puisque cette collecte est indolore, invisible, largement faite à notre insu, ou du moins sans que notre consentement ne soit réellement éclairé. L'écueil social enfin, quand le plus souvent les réactions des utilisateurs sont le désintérêt ou le fatalisme.

Pourtant, la surveillance et l'exploitation des données personnelles mettent en danger plusieurs de nos droits fondamentaux : tout d'abord le droit à la vie privée, à l'intimité. Ce droit qui nous permet de garder par-devers nous, ou pour les personnes que nous avons choisies, des opinions, des informations, des caractéristiques de notre vie qui nous sont propres et qui nous définissent. De ce droit à la vie privée découlent la liberté d'opinion et la liberté de croyance. Ces droits fondamentaux, dont le respect conditionne en grande partie l'appartenance à une démocratie, sont profondément mis en danger par la surveillance quand elle devient si généralisée qu'on l'intériorise naturellement : on risque alors de s'autocensurer, de restreindre ses fréquentations, ses recherches intellectuelles, politiques, religieuses, sexuelles, culturelles. Par peur que ces recherches en disent trop sur nous. Notre liberté d'information est également mise en danger lorsque toutes nos recherches sur internet sont tracées, froidement, et que les législations commencent, comme c'est le cas en France, à condamner la consultation elle-même de certains sites internet. Par le simple fait de voir l'intégralité de nos activités sur internet tracées et conservées, accessibles à de nombreuses entreprises et aux services de renseignement, nos droits les plus fondamentaux et notre intimité la plus profonde sont potentiellement ou concrètement auscultés et utilisés à des fins commerciales ou sécuritaires.

Si nous laissons se développer cette surveillance sans réussir à dépasser les écueils cités plus haut, il y a grand risque que nos sociétés connectées deviennent des sociétés de la méfiance, du non-dit et de l'autocensure, alors qu'internet promettait l'ouverture, les contacts et la découverte infinie. Ce serait un échec majeur et un danger grave pour la vitalité politique, culturelle, humaine de nos sociétés. Nous avons vu tout au long du xx e siècle les ravages des sociétés de contrôle basées sur la surveillance et le fichage des citoyens. Nous ne pouvons pas laisser la surveillance numérique détruire, avec une puissance bien supérieure, nos fragiles démocraties.

Il est donc crucial de s'atteler, comme l'a fait Tristan Nitot dans ce livre, à répondre à ces difficultés.

Expliquer d'abord, en détail et avec des exemples simples, ce que veut dire « collecter et exploiter des

données personnelles » dans l'espace numérique.

Faire comprendre les grands enjeux du modèle d'exploitation des données personnelles aujourd'hui dominant sur internet.

Éclairer les modalités et les objectifs de la surveillance commerciale aussi bien que de la surveillance étatique.

Mais ces explications ne peuvent se suffire, faute de quoi elles poussent au découragement et à ce fatalisme déjà trop répandu. Car c'est une constante : lorsqu'on prend conscience de l'étendue des données que nous laissons circuler, de ce que ces données disent de nous, et enfin de la manière dont elles sont exploitées, c'est un sentiment d'écrasement qui nous saisit. Comment faire pour se défendre contre des géants nommés Google, Apple, Microsoft, Facebook ou Amazon ? Faut-il se passer de tout ce qu'internet et le web nous ont apporté depuis vingt ans ? Renoncer aux liens sociaux que nous y avons créés, aux contenus et aux informations enfin accessibles, aux opportunités de développement intellectuel ou commercial ? Cela semble impossible, et cela nous couperait des merveilleuses opportunités de découvertes et de liens, par-delà les frontières et les restrictions d'antan. Alors accepter ce pillage permanent et invisible de notre intimité ? C'est le choix, ou plutôt le non-choix, que beaucoup font. Et la puissance des entreprises qui ont envahi notre quotidien crée en nous le sentiment que rien ne sert de vouloir se rebeller, que notre seul choix serait d'abandonner l'utilisation d'internet si nous voulons échapper à la surveillance. Ce qu'évidemment peu de gens sont prêts à faire.

C'est là que l'ouvrage de Tristan Nitot prend tout son sens : ne s'arrêtant pas à une description anxiogène de la réalité de la surveillance numérique, il propose des pistes de réflexion et d'action à la fois à titre individuel, mais également pour un changement plus important des modèles économiques, des outils et de la philosophie du développement d'internet.

Ce travail est absolument nécessaire, car nous ne pouvons accepter l'alternative infernale entre nous soumettre ou renoncer. Il est possible de développer à la fois une prise de conscience globale, des changements de comportement individuel, et d'imaginer des réorientations plus profondes, qui accompagneront et pousseront aux changements législatifs à venir.

Nous, utilisateurs d'internet, sommes souvent inconscients de notre pouvoir : en tant que citoyens nous pouvons, nous devons, demander à nos responsables politiques des législations protectrices face à la surveillance étatique comme commerciale (d'autant que la première se nourrit de plus en plus de la seconde). Nous devons faire de la protection de la vie privée et de l'intimité un enjeu politique au même titre que la protection sociale, les politiques économiques ou les relations internationales : il en va de la bonne santé démocratique de nos sociétés, et de la protection des individus.

En tant qu'utilisateurs de multiples services sur internet, nous avons également le pouvoir d'influer sur les modèles économiques, et donc sur la prédation de données personnelles, des entreprises dont nous sommes utilisateurs et clients. À nous de refuser d'utiliser des services qui nous font du tort, et de privilégier ceux qui nous respectent. Évidemment chacun se sent démuni lorsqu'il est seul, mais il ne tient qu'à une prise de conscience collective et une volonté d'agir pour que le respect de l'utilisateur et de son intimité deviennent des arguments et des atouts pour les services internet,

comme le sont l’aisance d’utilisation, l’ergonomie, le service rendu ou la gratuité.

Il y a mille façons d’aborder la question de la surveillance et des données personnelles. Celle qui est probablement la plus utile aujourd’hui est celle qui nous redonne le pouvoir d’agir. Celle qui fait le pari de proposer des pistes, certes partielles, mais qui redonnent du sens : il est très enthousiasmant de se voir jour après jour reprendre la main sur les outils qu’on utilise, comprendre les enjeux et faire des choix véritablement réfléchis. Quiconque a sauté le pas (de moins en moins coûteux) d’installer un système d’exploitation libre sur son ordinateur, de choisir en conscience tel ou tel service, ou de restreindre les traces qu’il laisse sur internet, a pu ressentir la satisfaction de cette reprise en main, ce sentiment d’être moins soumis à sa machine et de reprendre une part de pouvoir sur son quotidien. C’est l’approche du livre de Tristan Nitot, et en ce sens, elle est fondatrice.

C’est cette approche que les militants du libre et les défenseurs des libertés numériques devront développer dans les années qui viennent : offrir des explications claires et ouvertes des problèmes, en les adossant à des propositions concrètes pour les surmonter. Avec en permanence ce projet collectif comme horizon : travailler à un internet plus ouvert, plus libre, plus décentralisé, plus protecteur de ses usagers et plus facile à prendre en main par chacun.

Avant-propos

Tristan Nitot

Tristan Nitot est entrepreneur, blogueur et conférencier. Il est actuellement *Chief Product Officer* de Cozy Cloud. Il a été à l'initiative de la création de Mozilla Europe, qu'il a présidée. Tristan Nitot a été membre du Conseil National du Numérique (2013-2015), où il s'est concentré sur les libertés numériques et la neutralité du Net. Depuis septembre 2015, il est membre du comité de prospective de la CNIL.

Avez-vous déjà imaginé de renoncer à toute informatique pendant un mois ? Pas de mail, pas d'ordinateur, pas de smartphone, pas de wifi ? Pendant un mois entier ? Ou même une semaine ?

Il suffit d'essayer d'imaginer cela pour comprendre à quel point l'informatique et l'internet occupent dorénavant un rôle central dans nos vies. Nous utilisons ces outils pour nous tenir au courant de l'actualité, pour rester en contact avec nos proches même s'ils sont loin, pour nous distraire, pour vérifier la véracité d'une information sur Wikipédia (ou la copier/coller pour un devoir), pour savoir comment aller d'un point à un autre ou pour acheter en ligne.

Le temps où l'ordinateur était une affaire de spécialistes est maintenant bien loin, car l'informatique et internet nous touchent, nous qui sommes équipés, au quotidien. Mieux : il y a quelques années

encore, un ordinateur connecté à internet était une grosse boîte métallique avec un câble d'alimentation et un câble réseau. Aujourd'hui, il y a de fortes chances, cher lecteur, que vous ayez dans votre poche un ordinateur au moins aussi puissant que ceux de l'époque, alimenté sur batteries et connecté sans fil à internet. C'est de fait un ordinateur, même si on appelle cela plutôt un smartphone.

L'informatique a changé radicalement ces trois dernières décennies, et son omniprésence a transformé le rapport que nous avons avec elle. L'informatique est disponible alors que nous nous déplaçons, et nous avons accès à des ordinateurs rapides et des volumes de données de taille insoupçonnée il y a encore peu de temps. Je ne cesse de m'étonner d'avoir dans la poche une encyclopédie dans plusieurs langues, des cartes du monde entier, et un accès aux toutes dernières infos, parfois sur des sujets des plus pointus. Le progrès réalisé est formidable et les possibilités sans cesse croissantes continuent de m'émerveiller chaque jour. J'aime l'informatique, j'aime internet, et j'aime ce qu'ils me permettent de faire.

Pourtant, il y a comme un malaise.

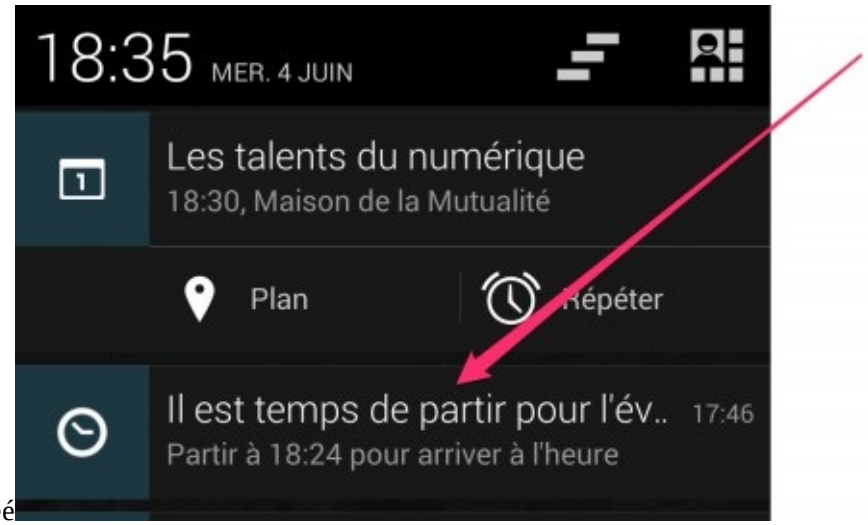
Récemment, j'ai eu une drôle d'impression en retrouvant sur de nombreux sites la photo d'un objet que j'avais envisagé d'acheter, comme si ce dernier me suivait. J'ai appris plus tard que c'était une technique de marketing appelée *retargeting* ou « reciblage publicitaire ». J'ai demandé à Wikipédia, qui m'a expliqué :

Le reciblage publicitaire (en anglais : *behavioral retargeting*, *behavioral search retargeting* ou simplement *retargeting*) consiste à afficher des messages publicitaires sous forme de bannières sur des sites internet après qu'un internaute ait fait preuve d'un intérêt particulier pour un produit sur un autre site.

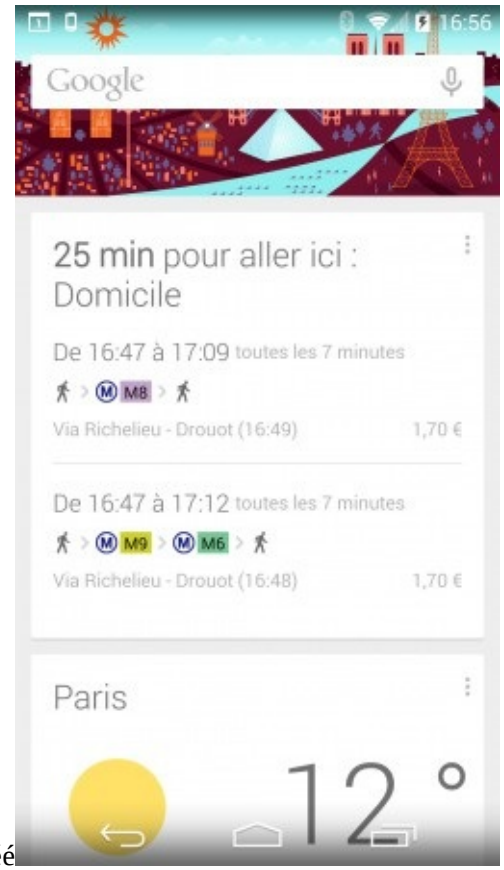
Ah, quel soulagement, je ne suis donc pas fou ! C'est mon ordinateur qui informe des sites marchands que j'ai déjà été intéressé par certains articles sur d'autres sites marchands… Tout d'un coup, je regarde mon ordinateur d'un œil méfiant.

Les choses se sont aggravées quand un beau jour mon téléphone m'a envoyé une alerte : « *Il est temps de partir pour l'événement* ». Mon téléphone avait pris l'initiative de regarder dans mon agenda l'heure et le lieu de mon prochain rendez-vous.

Il a ensuite pris l'initiative, sans que je ne lui demande rien, de se renseigner sur les horaires des métros et même le tarif des tickets pour me dire qu'il fallait rentrer chez moi.


18:35 MER. 4 JUIN
Les talents du numérique
18:30, Maison de la Mutualité
Plan
Répéter
Il est temps de partir pour l'év.. 17:46
Partir à 18:24 pour arriver à l'heure
éééé

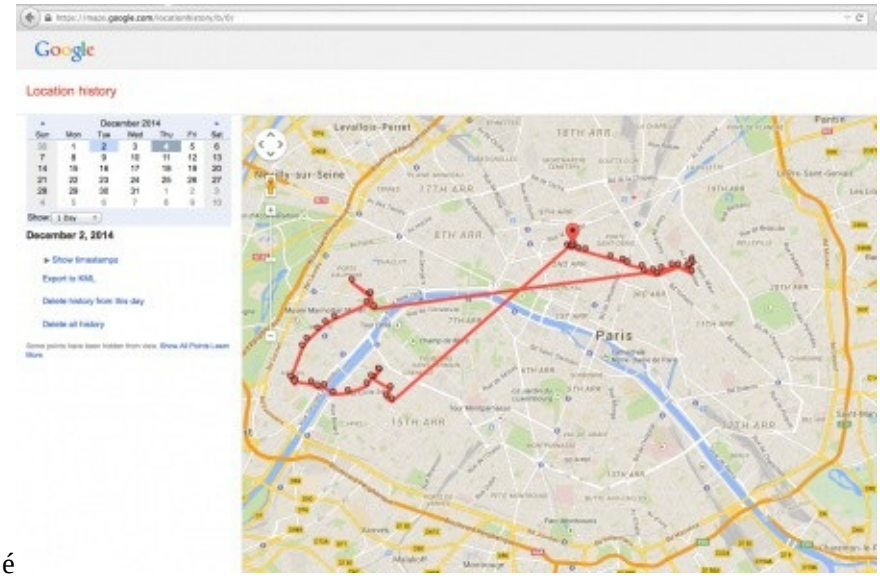
Capture d'écran d'un écran de téléphone portable : une notification de rendez-vous, et une notification de Google indiquant à Tristan Nitot qu'il est temps de partir pour ce rendez-vous.



éééé

Capture d'écran d'un écran de téléphone portable : indications concernant le trajet à effectuer pour se rendre à une adresse, et notification de la météo.

D’un côté c’est pratique, mais c’est aussi surprenant, et je n’ai pas le souvenir de lui avoir donné la permission de faire cela. J’ai effectué quelques recherches pour comprendre et j’ai entendu parler d’un service de Google appelé « Google Location Services ». J’ai cliqué sur le lien http://maps.google.com/locationhistory, et je suis tombé sur la carte suivante :

é 

Capture d'écran du service d'historique des déplacements de Google Maps, avec l'affichage des trajets de Tristan Nitot effectués le 2 décembre 2014.

La trace que l’on voit sur la carte, ce sont mes déplacements (ici, pour la date du 2 décembre 2014). Mon téléphone, connecté à Google et doté d’un GPS, me piste au quotidien et envoie mes déplacements en permanence quelque part sur un ordinateur chez Google. Mon ordinateur et mon téléphone sont toujours avec moi, savent tout de moi et certains logiciels qu’ils embarquent remontent ces informations à des ordinateurs dont j’ignore tout. Je suis surveillé en permanence, aussi bien pour mon usage de l’internet que celui de mon téléphone… sans avoir rien demandé ! Comme je le disais plus haut, je suis passionné d’internet et d’informatique, mais je réalise que ce n’est plus moi qui contrôle mon ordinateur ni mon smartphone.

C’est ce que je voudrais explorer dans ce petit livre : comment saisir le potentiel positif de l’informatique connectée sans devenir victime de la surveillance de masse. Au-delà des dénonciations, il me semble important de comprendre les ressorts de l’usage de nos traces, mais également de montrer les outils et les méthodes qui permettent de conserver une part de libre arbitre dans nos usages numériques. J’ai essayé de produire un ouvrage simple, instructif et compréhensible par tous et toutes. J’espère que vous prendrez plaisir à le lire.

Première partie

Souriez, vous êtes surveillés !

Les dangers de la surveillance

Première partie

Souriez, vous êtes surveillés !

Les dangers de la surveillance

1. Est-il si grave de perdre le contrôle de son ordinateur et de son smartphone ?

On vient de le voir, mon smartphone laisse fuiter des données (par exemple mes déplacements) et mon ordinateur fait de même avec la liste des pages web que je visite. Ces données sont envoyées à des sociétés que je ne connais pas forcément, et les logiciels que j'utilise font sans mon accord des choses que je ne comprends pas. D'un certain côté, ça tombe bien : même moi qui suis diplômé en informatique, je n'ai guère envie de me plonger dans les entrailles de tous les logiciels que j'utilise. En effet, ce qui est important pour moi comme pour l'immense majorité des gens, c'est de pouvoir utiliser mon ordinateur et mon smartphone, pas de les bricoler ! Bien souvent, on se fiche de savoir comment fonctionnent les choses. C'est comme ma voiture : je ne veux pas avoir à soulever le capot. Moins je le fais, mieux je me porte.

Pourtant, je constate dans les sondages que la majorité des internautes s'inquiète de la vie privée en ligne.

Selon un sondage Pew 1, 91 % des internautes américains considèrent qu'ils ont perdu le contrôle sur la façon dont les entreprises collectent leurs données personnelles, et 80 % des utilisateurs de médias sociaux se disent inquiets du fait que des tiers, comme les annonceurs publicitaires ou des entreprises, puissent récupérer les données qu'ils partagent sur ces sites.

Mozilla publiait récemment 2 les résultats d'un sondage réalisé dans plusieurs pays du monde, dont la France. Il en ressortait que 74 % des internautes considèrent que leurs informations sont moins protégées aujourd'hui qu'il y a un an. Le même pourcentage d'internautes adultes considère que les sociétés de l'internet en savent trop sur eux.

Clairement, il y a une forte inquiétude de nos contemporains quant au contrôle de nos données personnelles.

2. Les risques personnels

Celebgate

Les bévues liées au non-respect de nos vies privées sont légion. Le premier qui me vient à l'esprit est le scandale du *celebgate*, quand des célébrités, Jennifer Lawrence et Kirsten Dunst en tête, ont vu des photos confidentielles provenant de leurs smartphones publiées sur le net le 31 août 2014 3.

Cette situation constitue une bonne illustration de la nécessité du respect de vie privée : il n'y a rien d'illégal ni d'indécent à être nu, et à se prendre en photo devant sa glace. Mais rendre publiques de telles photos constitue une agression sexuelle, profondément perturbante. Il n'y a pas besoin de faire des choses illégales pour avoir besoin qu'elles restent confidentielles. Et cela s'applique à chacun de nous : je souhaite à tous mes lecteurs et lectrices d'avoir une vie sentimentale et amoureuse réussie, mais rares sont celles ou ceux qui voudraient voir publiées des photos exposant leur vie amoureuse dans les moindres détails. Encore plus prosaïquement, les verrous dans les toilettes existent pour protéger l'intimité de chacun, même si faire ses besoins naturels est justement ce qu'il y a de plus… naturel.

Le scandale du *celebgate* possède également un aspect pédagogique. En effet, la majorité des victimes n'avaient pas du tout réalisé que les photos prises avec leur iPhone étaient automatiquement envoyées aux serveurs d'Apple pour « sauvegarde » ou « synchronisation ». Des pirates ont mis la main sur ces sauvegardes et ont publié les photos. Même si les smartphones des victimes n'ont pas été volés ou piratés, les données (ici des photos intimes) ont été copiées sur des ordinateurs d'Apple où elles ont été piratées. Il faut bien comprendre qu'Apple, qui est une des sociétés les plus respectueuses de la vie privée, ne fait pas ces copies pour faire fuiter des données. Ce sont des copies de sauvegarde conservées chez Apple pour que l'utilisateur puisse les récupérer au cas où son smartphone serait perdu ou cassé. Certains ont reproché à Apple le manque de protection de ces sauvegardes. La marque à la pomme a depuis augmenté la sécurité de ses serveurs. Mais nul n'est à l'abri d'une autre faille de la sécurité informatique, ou d'un choix de mot de passe trop fragile.

Le *celebgate* ne doit pas être l'arbre qui cache la forêt. Les scandales liés au manque de protection des données par des sociétés qu'on pourrait croire sérieuses sont nombreux. Le journal *Los Angeles Times* a recensé quelques superbes bévues relatives à la vie privée en 2014 4.

ING et publicité

Au mois de mars 2014, la banque néerlandaise ING a décidé d'analyser les dépenses figurant sur les relevés de compte de ses clients 5. Le directeur de la branche « banque privée » d'ING s'est vanté sur son site d'être en charge de la plus grande quantité de paiements dans le pays et donc de savoir « *non seulement ce qu'achètent les gens, mais aussi où ils achètent* ». Ces informations ont été utilisées à des fins publicitaires, menant à un scandale qui a poussé la banque à faire marche arrière, et l'a contrainte à admettre que les données étaient la propriété des clients et non celle de la banque.

Uber et le mode « Vision de Dieu »

La société américaine Uber, qui offre des services de VTC (Véhicules de Tourisme avec Chauffeurs) concurrents des taxis, a une façon étonnante de distraire ses invités lors de soirées privées, en affichant sur grand écran les trajets des véhicules en cours, parfois avec les noms des passagers connus 6. Le suivi des véhicules et des occupants peut mener à des situations scabreuses, par exemple quand Uber s'amuse à suivre les gens qui vont en soirée à un endroit le samedi soir via un véhicule Uber et qui ne repartent de là-bas que le lendemain, toujours avec un véhicule Uber : Uber sait quels sont les clients qui ont découché suite à une soirée. Ces « trajets de la gloire », comme les appelle la compagnie, ont fait l'objet d'un article sur le blog de la société. L'article a été retiré depuis, compte tenu de l'outrage qu'il a causé : il est en effet très désagréable de réaliser que la compagnie de taxi que vous utilisez sait si vous avez « pécho »… et s'en vante sur son site web ! Et ça n'est pas le seul usage : Uber sait si ses clients se rendent régulièrement dans un hôpital spécialisé dans la lutte contre le cancer 7, ou dans un centre de planning familial ou chez un concurrent de leur employeur…

Mais la vraie question, c'est que les clients n'imaginent que très rarement que ces données existent. On imagine encore moins que ces données soient accessibles par n'importe quel employé Uber, ni l'impact que de telles informations peuvent avoir quand elles sont employées contre l'utilisateur, pour lui nuire.

Le podomètre mouchard

Il est une source de données qu'on ne soupçonne pas forcément, alors qu'elle est en plein essor. Je veux parler de ces objets connectés que l'on porte sur soi, les « *trackers* d'activité physique », des podomètres électroniques sophistiqués. Il existe différentes marques sur le marché, mais le principe général est le même : ils comptent les calories dépensées pendant la journée en fonction de nos mouvements, pour nous permettre d'atteindre des objectifs quotidiens. Les données sont transmises sans fil jusqu'à notre ordinateur ou notre smartphone et sont ensuite envoyées à un ordinateur serveur qui analyse ces données. J'en ai un moi même, et je reconnais que c'est efficace quand on a une vie sédentaire et qu'il s'agit de se motiver pour bouger.

Mais voilà, les données collectées ne sont pas forcément utilisées pour faire de l'exercice, mais peuvent l'être aussi dans des procès pour demander des dommages et intérêts. Un récent article du magazine *Forbes* 8 explique comment une jeune femme qui menait une vie active est devenue moins active depuis un accident de voiture. Pour prouver cela, les avocats de la jeune femme lui ont fait porter pendant plusieurs mois un bracelet de marque Fitbit qui mesure l'activité physique. Cela pourrait bien permettre à la jeune femme de toucher de copieux dommages et intérêts. Le souci, c'est que les assureurs demanderont un jour à accéder à ces données de façon à détecter si leurs clients ont une activité régulière, espérant ainsi augmenter le prix des assurances pour les gens qui bougent moins que la normale. Après tout, il est déjà courant de passer une visite médicale quand on contracte un emprunt important, alors pourquoi ne pas aller piocher directement chez les fournisseurs de podomètres électroniques ? On notera à cet effet qu'un assureur, AXA, distribue des podomètres Withings à ses nouveaux clients 9 et aura accès aux données de santé des utilisateurs (nombre de pas effectués par jour, rythme cardiaque, taux d'oxygène dans le sang et qualité du sommeil) s'ils

l'autorisent. Combien de temps avant que cela ne se généralise et que les assureurs ne fassent payer plus cher les clients qui refusent de porter un tel mouchard connecté ou ceux qui font moins de 10 000 pas par jour ?

Le smartphone

Le fait est que les sociétés de technologie savent beaucoup de choses sur leurs utilisateurs grâce à des données collectées pendant l'usage du service qu'elles proposent, même pour des services aussi simples qu'un taxi, un podomètre amélioré ou une banque.

Dans cette fuite des données, le smartphone n'est pas en reste, à en croire une récente étude de la CNIL (Commission Nationale Informatique et Libertés) qui a mesuré avec l'aide des informaticiens de l'INRIA que certaines applications piochaient allègrement dans nos données personnelles 10, avec une préférence pour les identifiants du téléphone (numéros uniques) et… la position GPS de l'utilisateur.

Comme le rappelle la CNIL :

« *Une base de données de localisation [permet] de déduire des informations détaillées sur les habitudes et modes de vie des personnes : lieux de vie et de travail, sorties, loisirs, mobilités, mais aussi éventuellement fréquentation d'établissements de soins ou de lieux de culte.* »

Indirectement, notre smartphone pourrait révéler nos pratiques religieuses, nos problèmes de santé et nos goûts en termes de loisirs ou de fréquentation de restaurants.

On notera que parmi les applications observées par la CNIL, une a accédé à la géolocalisation plus d'un million de fois en trois mois, soit plus d'une demande par minute. De leur côté, certains éléments des smartphones Android (par Google) ne font guère mieux :

L'application-widget « Actualités et météo » a accédé 1 560 926 fois à la localisation de l'utilisateur pendant les trois mois de l'expérimentation. Cette application a aussi communiqué 341 025 fois avec internet.

Le problème, comme le souligne la CNIL, c'est que :

Ces applications étant présentes par défaut sur l'appareil et ne pouvant être supprimées, l'utilisateur n'a pas pu consulter les informations collectées, qui sont généralement affichées avant le téléchargement et l'installation d'une application sur Android.

Un morceau de logiciel d'un smartphone qui cherche où l'on se trouve et qui se connecte de lui-même à internet toutes les 2,6 minutes pendant les trois mois de l'expérience sans que l'utilisateur ne sache ce qui est échangé en termes de données, voilà qui n'est guère rassurant…

La combinaison des données

Avec un *tracker* d'activité physique, nos changements physiologiques (rythme cardiaque, mouvements), sont mesurés et stockés « dans le cloud », c'est-à-dire quelque part sur un serveur d'une société privée. Cela signifie que cette société, pour peu qu'elle s'en donne la peine, peut déterminer facilement quand vous faites l'amour 11 : certains de ces *trackers* permettent déjà de mesurer les

différentes phases du sommeil. Une simple modification de l'algorithme permettrait de déterminer quand le sujet a des relations sexuelles.

Par ailleurs, comme démontré ci-dessus par la CNIL, nos smartphones savent en permanence où nous sommes. Cela n'est pas grave en soi, mais il est intéressant d'imaginer ce qui pourrait arriver si on combinait ces données… avec celles d'autres personnes. Ainsi, on pourrait savoir qui est le partenaire de qui, juste en regardant quelles coordonnées GPS et quels indicateurs de relations sexuelles correspondent. Ces données pourraient intéresser les assureurs (des relations sexuelles régulières seraient bénéfiques pour le cœur), mais pourraient aussi permettre de ficher les personnes ayant des relations extraconjugales ou homosexuelles.

De telles informations peuvent se révéler très utiles quand il s'agit de faire pression sur une personne pour des raisons politiques ou commerciales.

Heureusement, cette situation de combinaison de données n'est qu'imaginaire pour l'instant. Il y a quelques années, elle était juste impensable. Aujourd'hui, la plupart des éléments pour la rendre possible sont déjà en place…

3. Google sait tout sur nous, voici comment

Il est une société qui sait presque tout sur ses utilisateurs, car, comme elle l'explique elle-même 12 :

La mission de Google est d'organiser l'information du monde, de la rendre utile et accessible de partout.

La somme des informations que Google possède sur nous est inimaginable, car c'est sa « mission » de tout collecter. Du coup, dans la plupart de ses produits, du moteur de recherche à sa messagerie Gmail ou son outil statistique Google Analytics, tout est prévu pour en apprendre plus sur les internautes, leurs intérêts, leurs comportements et leurs données. Cela commence bien sûr par son produit phare, son moteur de recherche, qui a plus de 95 % de parts de marché en France 13.

Voici un récapitulatif très partiel des produits proposés par Google, avec les données qui sont collectées.

Produit	**Données collectées**
Google Search (moteur de recherche)	– Questionnements de l'utilisateur et ses centres d'intérêt, ses recherches commerciales ou de voyage.
Gmail	– Contenu des emails, y compris les pièces jointes, destinataires, contacts, fréquence des échanges.
Google Analytics (statistiques)	– Déplacement de l'internaute sur le web, liste des pages visitées, temps passé. Google peut pister les visiteurs de 88 % des sites web. – Il existe une version pour les applications mobiles permettant de suivre tout ce que fait un utilisateur au sein d'une application sur son smartphone.
Google Maps	– Lieux géographiques intéressant l'utilisateur, itinéraires prévus.
Smartphone Android	– Déplacements géographiques, vitesse de déplacement, carnet d'adresses, historique des appels téléphoniques, des SMS, applications installées.
Google Calendar	– Rendez-vous, lieux, dates, interlocuteurs, sujets de vos rendez-vous (personnels et/ou professionnels).
Google Wallet	– Numéro de carte bancaire, achats en ligne.
Google Docs & Drive	– Documents bureautiques (contenu de feuilles de tableur, textes, présentations…).
Google Chrome (navigateur)	– Mots de passe, historique des sites visités, temps passé sur les sites, fréquence de visite.
Google Photos	– Photos, lieux de prise de vue, date et heure de la prise de vue.
YouTube	– Vidéos vues, temps passé devant, moments où l'on fait pause, ce que l'on passe en boucle, vidéos qu'on veut regarder plus tard.

Google Private results (option de Google Search)	– Rendez-vous, factures à payer, livraisons en attente, vols en avion, réservations d'hôtels ou de restaurants.
Nest (Thermostat, détecteurs, caméras)	– Présence à la maison, température, qualité de l'air, consommation d'énergie.

Grâce à son moteur de recherche, Google connaît les questions que nous nous posons. Avec l'outil de mesure d'audience Google Analytics, le leader du secteur, Google sait quels sites nous visitons. Grâce aux téléphones Android (de marque Samsung, LG, Sony, HTC, etc.), il connaît nos déplacements. Grâce à Google Maps, il sait quels endroits nous envisageons de visiter. Grâce à Google Calendar, il sait avec qui nous avons rendez-vous, quand, et pourquoi. Grâce à Google Docs, il sait sur quoi nous travaillons. Grâce à Google Chrome, le navigateur, il sait quels sites nous visitons et le temps que nous y passons. Il a aussi accès à nos mots de passe, qui sont envoyés aux serveurs Google. Je pourrais mentionner la longue liste des produits Google et ce que cela donne à Google en termes de connaissance de ses utilisateurs, mais ce livre n'y suffirait pas.

Bref, Google sait presque tout sur nous, bien plus qu'on ne pourrait l'imaginer, comme l'atteste la liste ci-dessus. Il faut noter que nous donnons consciemment des données à Google, mais aussi qu'il en collecte sans que nous en ayons conscience, puis il recoupe ces données automatiquement entre elles pour les valider.

On se rassurera en se disant que oui, Google sait tout sur nous, mais nos informations sont bien protégées, Google, en qui nous avons confiance, les gardant pour lui… pour améliorer notre « expérience utilisateur ». Ou pas…

En effet, il existe au moins cinq raisons pour lesquelles ces informations pourraient fuiter au risque de pénaliser les utilisateurs. Passons-les donc en revue…

1er cas : Google dénonce volontairement l'utilisateur à la police

Dans certains cas, Google peut décider, après avoir analysé les données de l'utilisateur, de le dénoncer aux autorités de police. C'est ce qui est arrivé en août 2014 à un utilisateur de la messagerie Gmail 14.

En effet, ce Texan a envoyé via Gmail une photo pornographique d'une mineure en pièce jointe. Or, Google le dit lui-même dans ses conditions d'utilisation 15 :

Nos systèmes automatisés analysent vos contenus (y compris les e-mails) […]. Cette analyse a lieu lors de l'envoi, de la réception et du stockage des contenus.

Le pédophile texan a été dénoncé aux autorités qui l'ont arrêté immédiatement (ce dont on se félicitera !). Nul ne peut contester le bien-fondé du combat contre la pédophilie.

On peut cependant se demander ce qu'il va arriver quand Google va dénoncer des opposants à des régimes autoritaires après avoir lu leurs courriers et noté leurs centres d'intérêt…

C'est un sujet que nous aborderons dans un prochain chapitre. Mais pour l'instant, revenons aux différents scénarios relatifs aux données qui pourraient être mal utilisées.

2e cas : l'employé bizarre qui harcèle des enfants

On pourrait croire au scénario d'un feuilleton policier ordinaire, mais c'est malheureusement la réalité : un ingénieur de Google a utilisé son accès aux données privées des utilisateurs pour les harceler 16.

Évidemment, Google souhaite étouffer l'affaire pour ne pas faire peur aux utilisateurs, mais se doit en même temps de montrer que des mesures ont été prises contre l'employé en question. De ce fait, les détails sur l'affaire sont peu nombreux. On sait toutefois que l'ingénieur a accédé sans autorisation aux comptes Gmail et GTalk (messagerie instantanée) d'au moins quatre mineurs des deux sexes, utilisant les données trouvées pour faire pression sur ses victimes.

Contacté par la presse, Google s'est contenté d'affirmer avoir « *pris les mesures nécessaires* » mais « *ne peut pas en dire plus* ». Il semble qu'au moins un autre cas similaire ait déjà eu lieu 17 …

3e cas : Le piratage des serveurs

Nos données sont concentrées dans des « data centers », immenses hangars climatisés connectés à internet où sont alignés des ordinateurs qui traitent ces données. Cette concentration de données fait qu'un pirate réussissant à accéder au contenu de ces disques durs peut les recopier à distance.

De tels piratages arrivent fréquemment, et je vous propose d'en passer quelques-uns en revue pour se faire une idée du problème.

Parmi les sociétés qui ont été piratées, on trouve des grands noms comme eBay (on estime à 145 millions de comptes rendus publics), Adobe (152 millions de comptes compromis), les jeux Ubisoft, Apple (comptes de 275 000 développeurs d'applications), la Banque Centrale Européenne 18 et même… Domino's Pizza, qui a vu près de 600 000 comptes de clients français récupérés par des pirates qui demandaient une rançon de 30 000 €. Parmi les informations recueillies, le nom des clients, leur adresse, les instructions de livraison (code porte et interphone), et mots de passe. Domino's Pizza ayant refusé de payer, les maîtres-chanteurs ont publié ces données en novembre 2014 19.

La liste est très longue et les curieux pourront se référer au site http://informationisbeautiful.net.

La palme revient peut-être à Sony, qui a connu deux piratages successifs de grande envergure. Fin novembre 2014, un groupe de pirates appelé « Guardians of Peace » a pénétré le réseau informatique de Sony Pictures, la filiale de production cinématographique de Sony basée à Hollywood. Plus de 100 téraoctets de données ont été piratés, dont au moins cinq films qui ne sont pas encore sortis en salle, des scripts de films, les données personnelles (salaire) de tous les employés, parmi lesquels des acteurs comme Sylvester Stallone. Comme l'expliquent les patrons de la société, « *nous devons imaginer que toutes les données qu'avait l'entreprise sont potentiellement dans les mains de ceux qui nous ont attaqués* ».

Pourtant, Sony était déjà passé par un épisode dans le même genre, en 2011 avec sa filiale Sony Online Entertainment qui gère les jeux en réseau pour les consoles Playstation. Plus de 100 millions de comptes ont été concernés par cette attaque, dont au moins 10 millions contenaient les numéros de cartes bancaires des joueurs.

Au final, nombreux sont les experts en sécurité qui affirmeront qu'il y a deux types d'entreprises : celles qui ont été piratées et celles qui ne savent pas qu'elles l'ont été 20 … Certes, les serveurs de Google sont sûrement bien protégés mais ils ont aussi le défaut d'être particulièrement convoités par des personnes mal intentionnées car contenant des données sur à peu près tout le monde !

4e cas : les données sont siphonnées par les services secrets

Les documents du lanceur d'alerte Edward Snowden sur la NSA (National Security Agency) sont parfaitement clairs sur le sujet : certains services secrets, la NSA américaine et le GCHQ anglais ont mis en place plusieurs méthodes pour aller piocher chez Google et consorts des données personnelles. Nous détaillerons ceci dans le chapitre 6.

5e cas : Les données facilement accessibles par qui s'en donne la peine

Ce dernier cas est paradoxal, car le fait que les données soient visibles par quelqu'un de mal intentionné vient du fait… que l'utilisateur lui-même les a publiées, sans imaginer qu'elles seraient accessibles à d'autres. Il existe aujourd'hui sur internet de nouvelles nuisances comme le *doxing*, (de l'abréviation « docs » pour documents). Celui-ci consiste à accumuler des informations peu glorieuses relatives à une personne auprès de services en ligne comme Facebook, Twitter ou Instagram de façon à « monter un dossier » sur cette personne. Ensuite, il suffit de publier ledit dossier pour faire chanter la personne… sur la base d'informations qu'elle a elle-même rendues publiques.

4. Facebook, la manipulation des masses et la démocratie

Il est un cas de figure où des données personnelles peuvent être utilisées contre l'utilisateur sans même qu'elles ne quittent les ordinateurs de la société qui les détient. Facebook l'a démontré de façon brillante : des chercheurs ont utilisé le réseau social Facebook pour mener à très grande échelle une expérience psychologique à leur insu auprès de presque 700 000 utilisateurs. Cette expérience porte sur la façon dont Facebook filtre ce qui est affiché pour chacun. En effet, les utilisateurs du service reçoivent plus de contenu (photos, vidéos, messages, articles, publicités) qu'ils ne peuvent en consommer. Pour éviter la saturation des utilisateurs, Facebook n'affiche qu'une partie de ce contenu. Pour cela, il utilise un algorithme qui va faire des choix à la place de l'utilisateur. Cet algorithme est paramétrable : Facebook peut le modifier très simplement pour afficher différents types de contenu en fonction de ce qu'il sait de l'utilisateur, une connaissance obtenue par l'analyse des traces laissées par l'utilisateur lui-même ou par ses « amis ».

Dans le cadre de l'expérience qui nous intéresse, Facebook a choisi exactement 689 003 personnes et les a séparées en deux groupes. Au premier groupe, Facebook a surtout montré du contenu positif et joyeux (en retirant les mauvaises nouvelles), et le groupe a réagi en publiant des réactions plus positives que la moyenne. Au second groupe, Facebook a au contraire supprimé les messages positifs pour ne conserver que les messages négatifs et tristes. Très logiquement, l'humeur des cobayes involontaires du second groupe a été affectée de façon négative. De ce fait, ils ont répondu avec plus de messages négatifs. Facebook a mesuré cela en analysant le contenu des messages publiés par les utilisateurs.

Les chercheurs travaillant avec Facebook qui ont fièrement publié leurs travaux sur le sujet, avec le titre « *Preuve expérimentale d'une contagion émotionnelle à grande échelle par les réseaux sociaux* » [21] n'ont probablement pas anticipé une réaction aussi négative que celle qu'ils ont suscitée. En effet, l'idée de manipuler les émotions de 700 000 personnes sans les prévenir n'a pas vraiment été bien perçue, ni par les cobayes, ni par la presse.

Le problème ne s'arrête pas là. En novembre 2010, lors des élections dites *mid-term* aux USA, Facebook a lancé une autre expérimentation sur son service, visant à répondre à une question simple : « *un réseau social peut-il encourager les gens à voter ?* ». Facebook a donc mis en place un certain nombre de fonctionnalités pour ses utilisateurs américains en âge de voter : une image avec un lien menant vers une carte indiquant où trouver les bureaux de vote, un bouton permettant à l'utilisateur d'indiquer qu'il a voté, et les photos de profils de six amis ayant déjà voté.

L'expérience a porté sur 61 millions de personnes [22], soit quasiment la taille de la population française, et les résultats sont significatifs : on estime que 340 000 personnes supplémentaires [23] sont allées voter suite à la démarche de Facebook, ce qui est très sensible, compte tenu du fait que George W. Bush a remporté les élections présidentielles en 2000 à 537 voix près !

Il est louable de pousser les citoyens à voter, c'est sain pour la démocratie. Mais n'oublions pas que Facebook sait tout de nos intérêts, de nos lectures, et de nos opinions politiques. On peut sans peine

imaginer 24 ce qui arriverait si Facebook décidait de suivre la même procédure afin de favoriser un candidat par rapport à un autre, par exemple en incitant les électeurs qu'il sait proches de ce candidat à aller voter, tout en restant neutre auprès des électeurs de ses concurrents. Si l'élection est très serrée, Facebook pourrait tout à fait faire basculer les résultats dans un sens ou un autre.

Dans ce cas imaginaire, les données n'ont pas quitté les serveurs de Facebook, mais elles ont été utilisées contre la démocratie, à l'insu des utilisateurs, avec l'aide de leurs propres données…

5. La surveillance des États

Il y a quelques années, je discutais de surveillance des citoyens avec un fonctionnaire de police français. Il m'expliquait en substance que les citoyens craignaient les services de renseignement (renseignements généraux, DST, devenus DCRI puis DGSI). Il m'affirmait qu'en fait ces services en savent beaucoup moins sur chacun de nous que les grands services en ligne et les réseaux sociaux tels Google, Facebook ou encore Amazon et Apple. En effet, il est bien plus efficace de collecter les informations que les gens partagent volontairement que d'essayer de les espionner dans leur vie réelle.

Qu'à cela ne tienne, pour augmenter l'efficacité des services de renseignements, il suffirait qu'ils espionnent également les réseaux sociaux ! Cela pourrait être une boutade, mais c'est malheureusement la triste réalité. On s'en doutait depuis une quinzaine d'années avec l'affaire Echelon à la fin des années quatre-vingt-dix 25.

Mais c'est surtout en juin 2013 que le grand public a commencé à comprendre l'ampleur de la surveillance généralisée avec les révélations du lanceur d'alerte américain, Edward Snowden, un informaticien qui a travaillé dans une entreprise de sous-traitance pour différents services secrets américains : la CIA (Central Intelligence Agency, agents secrets américains sur le sol étranger) puis la NSA (National Security Agency).

Edward Snowden s'est réfugié à Hong-Kong, emportant avec lui des centaines de milliers de documents de la NSA classés « secret-défense » portant sur les programmes de surveillance d'internet et des outils de communication utilisés par l'agence américaine. Il a invité deux journalistes, Laura Poitras et Glenn Greenwald, à qui il a remis ses documents. Les deux journalistes ont ensuite analysé et publié les documents d'Edward Snowden. Glenn Greenwald en a d'ailleurs fait un livre passionnant, *Nulle part où se cacher* 26 et Laura Poitras a sorti en novembre 2014 *Citizenfour*, un documentaire largement récompensé 27.

Les révélations de Snowden sont telles qu'il faudrait plusieurs livres pour tout décrire, aussi vais-je me contenter de ne lister dans le tableau suivant que quelques programmes d'espionnage de la NSA et de ses alliés, dont le GCHQ anglais.

Ce tableau n'est qu'un tout petit extrait des programmes de surveillance de la NSA révélés par Edward Snowden, parmi les 446 programmes relevés par le site http://NSA-Observer.net.

Nom de code	**Cible**	**Surveillance**
Muscular	Yahoo! et Google via les câbles en fibre optique entre les centres de données.	– Contenu des emails des utilisateurs : texte, audio, vidéo et métadonnées (heure, émetteur, destinataires, sujet).
XKeyScore	« collecte quasi-systématique des activités de tout utilisateur sur Internet » dans plusieurs	– Comportement et données des utilisateurs.

	dizaines de pays, dont la majeure partie des pays européens, le Brésil, la Russie, l'Inde et la Chine. 700 serveurs sont répartis sur plus de 150 sites.	– Activité sur les médias sociaux (dont Facebook), y compris pour lire les messages privés. – Historique des sites visités – Mots clés utilisés sur les moteurs de recherche – Contenu des formulaires remplis par l'utilisateur, y compris les mots de passe.
BullRun	Systèmes de chiffrement dans le monde.	– Toute communication chiffrée, qui est donc considérée comme confidentielle ou potentiellement dangereuse.
OpticNerve	Webcam des utilisateurs de Yahoo Messenger.	– Capture toutes les 5 secondes d'une image issue de la webcam des utilisateurs lorsqu'ils communiquent via le logiciel Yahoo Messenger.
Tempora	Plus de 200 câbles internet sous-marins.	– Tout le trafic internet est surveillé conjointement par GCHQ (UK) et la NSA (USA).

Quand on les analyse, on remarque que les attaques de la NSA sur l'informatique mondiale se focalisent sur un certain nombre de points vulnérables : les câbles sous-marins et quelques très grands services utilisés par des centaines de millions d'utilisateurs. Ces services commerciaux (Facebook, Yahoo!, Google, Apple, Microsoft, etc.) collectent des données auprès de leurs utilisateurs et il suffit alors à la NSA d'aller récupérer ces données directement auprès de ces sociétés, avec ou sans leur consentement. Ces grandes sociétés sont *de facto* complices des services d'espionnage américains, probablement à leur corps défendant, soit parce que l'arsenal juridique les oblige à répondre aux demandes des services secrets, soit parce qu'ils sont eux-mêmes espionnés par ces services.

6. Big Data et grosses responsabilités

On entend souvent parler de *big data* sans toujours bien cerner de quoi il s'agit. En français, on devrait utiliser le terme de « mégadonnées ». Ce sont des ensembles de données gigantesques comme en collectent par exemple Twitter (7 téraoctets par jour) et Facebook (10 téraoctets). Rappelons qu'un téraoctet est l'équivalent de 1 000 milliards de caractères. Sachant que si on numérisait la Library of Congress, la plus grande bibliothèque du monde, on obtiendrait 18,75 téraoctets de données. Autrement dit, chaque jour, Twitter et Facebook produisent à peu près autant de données que ce que contient la plus grande bibliothèque du monde, à 10 % près. Les données de Facebook et de Twitter sont les données que produisent ou échangent les utilisateurs.

On a ici affaire à un véritable océan de données qu'il est possible d'explorer pour y trouver des informations particulièrement intéressantes. Les capitaines de ces navigations au sein des données sont appelés en anglais *data scientists*, genre de mathématiciens et statisticiens dont le métier est de découvrir et interpréter le sens de ces données non-structurées dans l'objectif d'en extraire de la valeur.

Comme tout cela peut sembler bien abstrait, voici un exemple tiré d'un contexte bien plus terre à terre, celui des supermarchés. Dans une interview de début 2012, un *data scientist* américain employé de la chaîne de grands magasins Target, racontait une anecdote amusante sur son métier 28 :

Un homme passablement en colère entre dans un supermarché Target près de Minneapolis (Minnesota, USA) et exige de parler au directeur : « Ma fille a reçu votre prospectus par la poste », dit-il. « Elle est encore au lycée, et vous lui envoyez des coupons de réduction pour des vêtements pour bébés et des berceaux ? *Mais vous voulez l'encourager à tomber enceinte à son âge ?* »

Le directeur tombe des nues. Il regarde le prospectus, qui porte bien le nom de la jeune cliente et contient des publicités pour des vêtements de femme enceinte, de quoi équiper une chambre de bébé et moult photos de bébés souriants. Très ennuyé, le directeur présente platement ses excuses et prévoit de rappeler le client un peu plus tard (aux États-Unis, la notion de service client va beaucoup plus loin qu'en France).

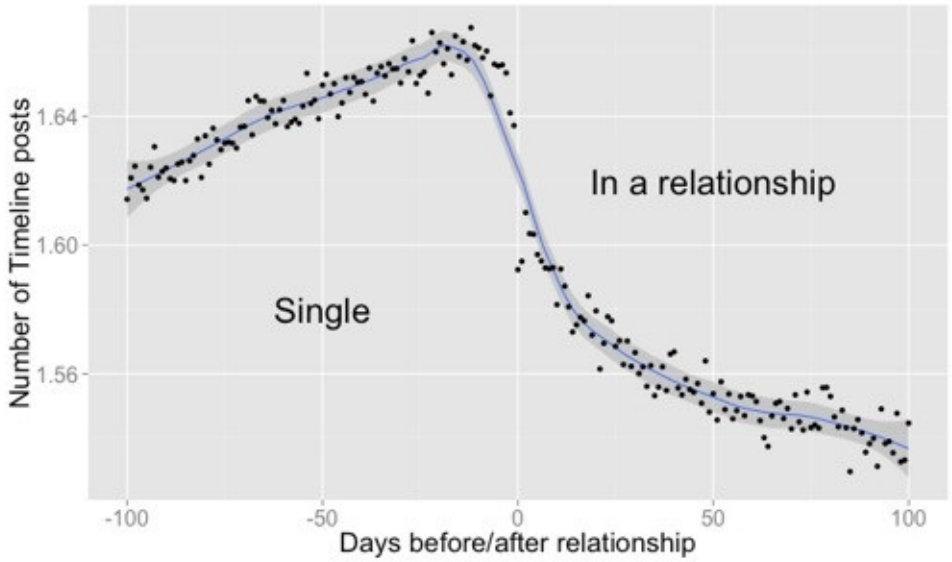
Quelques jours plus tard, le directeur appelle donc son client, mais le père de la lycéenne semble très décontenancé : « j'ai eu une conversation avec ma fille et… il s'avère qu'il s'est passé des choses pendant que j'avais le dos tourné… Voilà… Elle va accoucher au mois d'août. Je me dois de vous présenter des excuses ! »

Le rapport avec les *big data* ? Il est direct : la jeune fille, soit parce qu'elle payait avec une carte de paiement, soit avec une carte de fidélité, avait laissé un historique d'achats. Et les mathématiciens de Target ont remarqué que les achats de certains produits étaient corrélés avec une grossesse. Les lotions sans parfum en grands flacons (surtout au début du second trimestre de grossesse), les suppléments alimentaires à base de calcium, zinc et magnésium (à partir de la vingtième semaine de grossesse) et, juste avant l'accouchement, les grands sacs de coton hydrophile et de lingettes, sont autant de signaux que les statisticiens ont retenus et recherchent dans l'océan de données que nous

alimentons en permanence sans même le savoir.

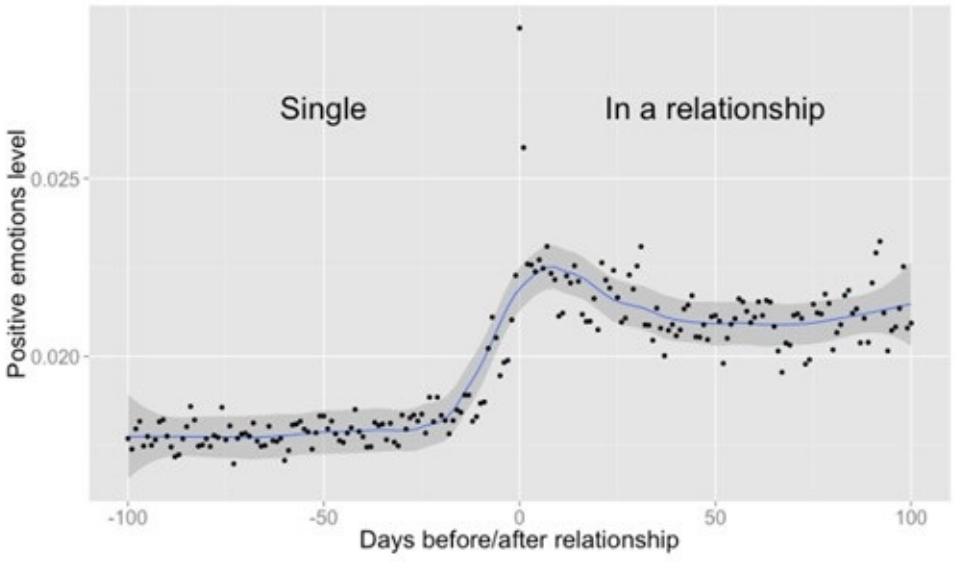
Un autre exemple, tiré du très officiel blog *Facebook Data Science* 29, sur un sujet où on n'attend guère les mathématiciens : le moment où l'on tombe amoureux.

Pour la Saint Valentin 2014, Facebook a en effet publié un long billet expliquant ce que l'on peut observer quand deux utilisateurs tombent amoureux et entament une relation sentimentale 30. Pour cela, Facebook a sélectionné les gens qui ont indiqué « avoir une relation » associé avec une date d'anniversaire pour cette relation. On observe ainsi que pendant la période de séduction, il y a de plus en plus d'interactions (messages échangés) entre les futurs partenaires via Facebook, mais que quelques jours avant de commencer la relation, le nombre de messages chute brusquement… pour ne pas remonter. Les mathématiciens de Facebook estiment que c'est dû au fait que les utilisateurs passent plus de temps ensemble dans le monde réel. Cela fait que Facebook est donc capable de prédire avec qui nous sommes en train de tomber amoureux, rien qu'avec nos données, avant même que cela ne soit devenu une réalité !



Facebook : déclin du nombre de posts lors du changement de statut de « célibataire » à « en couple ».

Ensuite, un graphique montre que les messages envoyés sont sensiblement plus positifs en moyenne après le début de la relation :



Facebook : augmentation de l'expression de sentiments positifs lors du changement de statut de « célibataire » à « en couple ».

Les deux exemples choisis ici, Target et Facebook, démontrent que le *big data* touche aussi bien le commerce que la sphère intime. Cela démontre également que les données qui alimentent le *big data* peuvent être captées auprès des utilisateurs sans que ceux-ci n'en aient la moindre idée : la carte bancaire ou de fidélité dans le cas de Target, ou le compte Facebook suffisent à ces sociétés pour construire des « profils » de chaque client-utilisateur, avec des implications qui peuvent être inattendues, surtout quand ces données sont piratées, ou revendues ou siphonnées par des services secrets.

7. L’impact de la surveillance sur la société

Il est une question à laquelle j’avoue avoir du mal à répondre : « *pourquoi la surveillance de masse est-elle néfaste à la société dans son ensemble ?* ». Comme beaucoup, j’ai une réponse viscérale à cette question : je sens que la surveillance de masse est mauvaise. Elle me révolte. Mais dès qu’il s’agit d’y répondre clairement, les choses se compliquent grandement. Aussi, j’ai dû replonger dans des cours de philo et de droit pour mettre des mots en réponse à cette question fondamentale.

Une idée qui a presque deux mille ans

Il se trouve que le problème est présent depuis longtemps. Depuis la Rome antique en fait. Le poète Juvénal écrivait dans ses satires « *mais qui va garder ces gardiens ?* » (« *sed quis custodiet ipsos custodes ?* »), phrase souvent utilisée pour parler des gouvernements qui surveillent les citoyens, puis qui a été étendue au problème de la surveillance de masse.

Le panoptique de Bentham

La réflexion sur la surveillance doit beaucoup au philosophe anglais Jeremy Bentham (1748-1832), inventeur du « panoptique », un modèle de prison circulaire avec une tour centrale où sont logés les gardiens. Depuis cette tour, les gardiens peuvent observer les détenus qui sont enfermés dans des cellules individuelles, sans que ceux-ci ne puissent savoir si on les observe. L’idée est de créer chez les prisonniers le sentiment qu’ils sont observés en permanence par des gardiens, qui savent tout sur eux, même quand les gardiens sont absents.

Il faut noter que Samuel Bentham, le propre frère de Jeremy Bentham, avait quant à lui dessiné des plans d’usines selon le même principe, pour surveiller les ouvriers et pas seulement des prisonniers.

Prison modèle à Cuba, construite sur le principe du panoptique en 1928 31.

En faisant croire aux gens qu'ils sont observés en permanence, on arrive à leur imposer une façon de se comporter.

Le philosophe français Michel Foucault (1926-1984) a critiqué le concept de panoptique dans son livre *Surveiller et punir* paru en 1975. Il analyse d'autres lieux que la prison et l'usine, comme par exemple l'école et l'hôpital, à la lumière de ce concept. Un élargissement qui fait dire au philosophe Gilles Deleuze (1925-1995) :

La formule abstraite du Panoptisme n'est plus « voir sans être vu », mais « imposer une conduite quelconque à une multiplicité humaine quelconque. »

Voilà, tout est dit : en faisant croire aux gens qu'ils sont observés en permanence, on arrive à leur imposer une façon de se comporter.

La vision de Glenn Greenwald et de Bruce Schneier

Glenn Greenwald et Bruce Schneier ont grandement influencé ma façon de penser sur ce sujet. Plutôt que de paraphraser leurs discours respectifs, je propose de traduire quelques extraits que voici.

Je laisse d'abord la parole à Glenn Greenwald, l'un des journalistes ayant permis les révélations d'Edward Snowden, avec deux extraits d'un discours qu'il a prononcé à la conférence TED d'octobre 2014 32 :

Il est important pour être un humain libre et heureux d'avoir un endroit où l'on peut se soustraire au regard et au jugement des autres. Il y a une raison pour laquelle nous cherchons tous cet endroit, c'est que nous tous, et pas seulement les terroristes et les criminels, avons des choses à cacher. Il y a toutes sortes de choses que nous faisons et pensons et que nous partageons avec notre médecin, notre avocat, notre psychologue, notre conjoint ou notre meilleur ami, choses qui nous humilieraient terriblement si le reste du monde venait à les savoir. De ce fait, pour chaque chose que nous faisons ou pensons, nous prenons la décision de la partager ou non avec notre entourage ou en ligne. Certains peuvent nier verbalement l'importance de la vie privée, mais le fait est que leurs actions prouvent le contraire. Il y a une raison pour laquelle l'intimité est si importante pour tous et de façon instinctive […] : quand nous sommes surveillés, écoutés, notre comportement change du tout au tout. […] Une société dans laquelle les gens peuvent être surveillés à tout moment est une société qui pousse à la conformité, l'obéissance et la soumission, et c'est pourquoi tous les tyrans recherchent un tel système. À l'inverse, et c'est plus important encore, c'est uniquement dans le cadre de la vie privée, de l'intimité, quand nous avons la possibilité d'aller quelque part où nous pouvons penser, raisonner et interagir sans le jugement ni le regard des autres, que nous pouvons explorer, être créatifs et exprimer notre dissidence. C'est pourquoi, si nous acceptons de vivre au sein d'une société dans laquelle nous sommes surveillés en permanence, nous acceptons de fait que l'essence de la liberté humaine soit complètement bridée.

Glenn Greenwald ajoute :

La surveillance de masse crée une prison dans l'esprit qui est bien plus subtile mais bien plus efficace pour favoriser la conformité aux normes sociales, bien plus effective que la force physique ne pourra jamais l'être.

Je laisse la conclusion à Bruce Schneier, un écrivain, cryptologue et expert en sécurité reconnu, dans

un billet qui date déjà de 2006 33 :

On considère trop souvent que le débat porte sur le choix entre sécurité et vie privée. Mais le véritable choix c'est la liberté par rapport au contrôle. La tyrannie, qu'elle vienne d'une attaque étrangère physique ou d'une scrutation permanente du pouvoir de l'État, c'est toujours la tyrannie. La liberté exige la sécurité sans intrusion. La surveillance policière est la définition même d'un État policier. C'est pour cela que nous devons défendre la vie privée même si nous n'avons rien à cacher.

8. Loi et vie privée

Parce qu'ils savent que la vie privée est un ingrédient fondamental pour être libre, les législateurs ont depuis longtemps souligné son importance, en l'inscrivant dans la loi. Voici un rapide tour d'horizon de ces textes, avant de voir comment la vie privée est essentielle pour que le citoyen puisse avoir confiance dans les institutions.

La Déclaration Universelle des Droits de l'Homme

En 1948, à la sortie de la Seconde Guerre mondiale, l'assemblée générale des Nations Unies adopte un texte d'orientation, à l'époque sans réelle portée juridique 34, la *Déclaration Universelle des Droits de l'Homme*.

Article 12 : Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

La Convention européenne de sauvegarde des droits de l'Homme et des libertés

La Convention européenne de sauvegarde des droits de l'Homme et des libertés, représente un progrès sensible en termes de force du texte, dans la mesure où il s'agit d'un traité international signé par les États membres du Conseil de l'Europe. Signée le 4 novembre 1950, elle est entrée en vigueur le 3 septembre 1953.

Article 8 : Toute personne a le droit au respect de sa vie privée.

La Charte des droits fondamentaux de l'Union Européenne

Cette charte n'a pas eu au départ de valeur juridique forte. Votée en décembre 2000, il aura fallu attendre le traité de Lisbonne en 2007 pour lui donner une valeur juridiquement contraignante dans les 27 états membres de l'Union Européenne.

Article 7 : Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.
Article 8 : Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

Les CNIL européennes

Enfin, en décembre 2014, l'ensemble des autorités indépendantes européennes concernées par les libertés dans une société informatisée (la CNIL française et ses homologues européennes), sous le nom de « groupe de l'article 29 » publiait une déclaration 35 très claire sur la protection de la vie privée :

Article 6 : La surveillance secrète, massive et indiscriminée de personnes en Europe […] n'est pas conforme aux Traités et législations européens. Elle est inacceptable sur le plan éthique.
Article 7 : L'accès à des données à caractère personnel aux fins de sécurité n'est pas acceptable dans une société démocratique dès lors qu'il est massif et sans condition.

Le cas des États-Unis

Aux États-Unis, c'est le quatrième amendement de la constitution, datant de 1792, qui protège la vie privée. Bien sûr nulle mention de numérique ou de données personnelles dans ce document ! Un peu moins d'un siècle plus tard, en 1890, deux juristes américains publiaient un article fondateur, « The Right to Privacy » 36. Mais ce n'est qu'en 1967, avec la jurisprudence « Katz v. United States 37 », que la notion de vie privée a été considérée comme découlant de ce quatrième amendement.

La confiance du citoyen dans les institutions

Pavel Mayer, membre historique du Parti Pirate allemand, explique 38 mieux que je ne pourrais le faire pourquoi le non-respect de la vie privée est toxique pour la démocratie :

La surveillance a des effets néfastes. Les citoyens croient à la liberté. Lorsqu'ils apprennent qu'ils ont été espionnés, alors ils perdent foi dans la société et dans les politiques. Et bientôt ils risquent d'oublier que les politiques sont élus par les citoyens, et sont au service des citoyens. Mais globalement, les deux sont liés. Avec Snowden, on a compris que quand une société commerciale collecte des données sur un individu, ces dernières peuvent être récupérées sans mal par les services secrets.

Cette réflexion est partagée par Daniel Solove, juriste américain et l'un des spécialistes mondiaux de la vie privée, pour qui l'érosion de la vie privée a des conséquences qui ressemblent plus au *Procès* de Franz Kafka qu'à *1984* de George Orwell. Dans ce livre, Orwell démontre comment une surveillance permanente empêche toute liberté, toute créativité et pousse tout le monde au conformisme dans une immense prison mentale.

Dans *Le Procès*, Franz Kafka raconte l'histoire d'un certain Joseph K. dont la vie est bouleversée par un procès sans qu'il ne soit jamais mis au courant du motif pour lequel il est jugé.

Pour Daniel Solove, c'est le manque de transparence de l'utilisation qui est faite de nos données qui pose un problème. Les données affectent les relations de pouvoir entre le citoyen et l'État. Ces relations sont frustrantes pour l'individu car elles créent chez lui un sentiment de totale impuissance et de faiblesse. Par ailleurs, elles affectent les relations qu'entretiennent les gens avec les institutions qui prennent des décisions importantes pour eux.

L'approche de Solove, focalisée sur l'État, qui fait la loi et sur l'importance de comprendre ce que l'État décide pour le citoyen, peut être confrontée à celle de Lawrence Lessig. Ce dernier, comme nous le verrons un peu plus tard, examine l'importance juridique de ce qui est programmé à l'intérieur du système informatique dans notre ère numérique : « *le code, c'est la loi* » (*Code is Law*).

Aujourd'hui, ce sont les grands acteurs commerciaux qui contrôlent le code et donc nos données qui peuvent décider, pour nous utilisateurs, ce que nous avons le droit de faire. Comment puis-je avoir

confiance dans les sociétés commerciales qui me fournissent des services, si je ne comprends pas comment elles prennent des décisions me concernant ? Comment vais-je réagir face à Facebook qui cache certains messages de mes amis et m'en montre d'autres sans que je sache pourquoi ? Comment vais-je réagir face à une mutuelle d'assurance qui refuse de m'assurer ou augmente ma cotisation parce qu'elle pense que je consomme trop de pizzas, de bières et de café mais pas assez de légumes verts ?

9. Mais, je n'ai rien à cacher !

Je ne peux pas finir cette réflexion sur l'importance de la vie privée sans aborder la réponse trop souvent faite par ceux qui ne comprennent pas les enjeux : « je n'ai rien à cacher ».

Faites ce que je dis, pas ce que je fais

Eric Schmidt, à ce moment-là président-directeur de Google, affirmait à la télévision américaine CNBC [39] « *S'il y a quelque chose que vous voudriez que personne ne sache, peut-être que vous devriez commencer par ne pas la faire* ». Dans le même registre, Mark Zuckerberg, PDG de Facebook, déclarait en 2010 [40] : « *Les gens ont pris l'habitude non seulement de partager plus d'informations de toutes sortes, mais ils le font de façon plus ouverte et avec plus de gens.* » Il ajoutait que la vie privée n'est plus la « norme sociale ».

Pourtant, si tous deux semblent penser que la vie privée ne devrait pas exister, ils protègent farouchement la leur ! Ainsi, le site CNet a révélé des informations sur Schmidt dans un article, ce qui leur a valu d'être mis sur la liste noire du service de presse de Google. Google ne répond donc plus aux questions de CNet. Le plus drôle, c'est que les informations publiées par CNet sur le patron de Google… avaient été obtenues en utilisant le moteur de recherche de Google, en moins de trente minutes !

Mark Zuckerberg, pour sa part, a acheté une belle maison à Palo Alto, Californie, où l'immobilier est particulièrement cher. Mais pour être sûr de ne pas être dérangé, il s'est aussi offert les quatre maisons adjacentes [41]. Coût total : environ trente millions de dollars !

Pour rester dans le registre immobilier, on apprend qu'Eric Schmidt vient d'acheter un appartement à New York [42]. Au-delà du prix (quinze millions de dollars tout de même), Eric Schmidt aurait choisi cet appartement car il dispose d'un ascenseur particulier et que contrairement à tout ce que veulent les New-Yorkais, il n'y a pas de concierge qui pourrait voir qui vient pour des rendez-vous galants, qui sont, semble-t-il, multiples [43].

Comme le fait ironiquement et très justement remarquer Cory Doctorow à Eric Schmidt [44] :

Dis, Eric, si tu ne veux pas qu'on sache combien tu gagnes, où tu vis et ce que tu fais de ton temps libre, peut-être faudrait-il ne pas acheter de maison, ni gagner un salaire, ni avoir des loisirs ?

Passons maintenant en revue les quatre raisons pour lesquelles l'affirmation « je n'ai rien à cacher » ne tient pas debout.

On a tous quelque chose à cacher

Nous avons tous des secrets. Pas forcément honteux. On ferme le loquet aux toilettes. On a des rideaux aux fenêtres de la chambre à coucher. On cache son code de carte bleue et son mot de passe d'email. Rares sont ceux qui aimeraient que le monde sache de qui ils étaient amoureux au collège ou au lycée. Je suis fier d'être papa de mes deux enfants, Robin et Philippine, mais je ne souhaite pas rentrer dans

les détails quant à leur conception… On a parfois envie de changer de travail sans que son employeur soit au courant. Les raisons sont multiples, et rien de ce que je viens de lister n'est illégal. Pourtant, on a, à chaque fois, une bonne raison de vouloir le cacher.

Chanter sous la douche

Avez-vous remarqué que l'on chante sous la douche quand on est seul, mais si une personne que l'on connaît mal peut nous entendre, cela nous fait souvent taire. Pourquoi ? C'est la peur du ridicule. C'est en substance ce que j'ai décrit dans le chapitre 7 : se sentir surveillé nous pousse à la conformité. Et pourtant, avant de pouvoir se lancer dans une prestation crédible de karaoké avec les collègues ou les amis, il faut avoir passé du temps à chanter mal, pour enfin progresser. Si on se sent surveillé, on s'autocensure, et on ne commence jamais à chanter. Je prends ici l'exemple de la chansonnette, mais on pourrait étendre la problématique à des choses plus sérieuses, comme l'art en général, l'expérimentation liée à des idées sur des sujets importants comme la politique, ce qu'on a vraiment envie de faire dans la vie ou la créativité en général, qui passe par une longue phase d'essais/erreurs.

Le secret commercial

Le monde des affaires a grand besoin de secret pour tout ce qui concerne les négociations de conditions commerciales ou les secrets de fabrication. Même si la NSA prétend agir contre le terrorisme, un fléau qu'il faut combattre, il apparaît qu'elle joue également un rôle très important dans l'espionnage économique. Son programme BLARNEY [45] nous montre que la NSA poursuit trois objectifs : la lutte contre le terrorisme, l'aide aux négociations diplomatiques et l'espionnage économique.

Dans les documents de Snowden sur le programme BLARNEY, parmi les « clients » de la NSA, figurent en bonne place les ministères de l'agriculture, des finances et du commerce des États-Unis, qui n'ont rien à voir avec la lutte contre le terrorisme.

De fait, toute société faisant du commerce a des choses à cacher (des tarifs, des méthodes de fabrication, sa liste de clients…), choses qui sont susceptibles d'intéresser des concurrents et/ou des services secrets de pays étrangers.

Les lois peuvent changer

Ce point est le plus difficile à accepter, car c'est celui qui évoque les perspectives les plus sombres, perspectives qu'on voudrait tous croire impensables. Les lois, sous l'impulsion de politiques qui réagissent à des événements, peuvent changer du tout au tout.

Un exemple : en 1940, en Alsace, parler français en public pouvait mener à plusieurs mois d'internement en camp « dont les conditions ne sont pas moins dures que dans les camps d'internement du Reich » [46] alors que la langue française était d'usage courant.

Bien sûr, j'espère de tout cœur que l'on ne reverra jamais de telles horreurs, mais l'histoire prouve que les lois peuvent changer avec une rapidité que l'on sous-estime. Ainsi, entre le début de la rédaction de cet ouvrage (décembre 2014) et sa remise à l'éditeur (juillet 2016), suite aux attentats de 2015 (Charlie Hebdo en janvier et le Bataclan en novembre) la France a vu arriver des lois sur la

surveillance de masse et la déchéance de nationalité, et l'état d'urgence a été déclaré par le président Hollande. On a ainsi vu un maraîcher bio se faire perquisitionner pour avoir des velléités écologistes 47 ou un homme assigné à résidence par erreur pour avoir téléphoné près des locaux de Charlie Hebdo 48.

Conclusion

On le voit, même si l'argument « je n'ai rien à cacher » peut sembler plein de bon sens au premier abord, il ne résiste pas à la réflexion. Il appartient à chaque défenseur des libertés et donc de la vie privée de savoir répondre à cet argument et à chaque citoyen de garder à l'esprit qu'il a quelque chose à cacher.

Notes

1 « Perceptions par le public de la vie privée et de la sécurité dans une ère post-Snowden », *Pew Research Center*, 12 novembre 2014 – http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

2 « Voici Polaris, une initiative destinée à améliorer la vie privée de chacun en ligne », *Mozilla*, 10 novembre 2014 – https://blog.mozilla.org/netpolicy/2014/11/10/introducing-polaris-privacy-initiative-to-accelerate-user-focused-privacy-online/.

3 Cet événement a donné lieu à une couverture presse phénoménale, mais c'est encore Wikipédia qui en fournit la meilleure synthèse : https://en.wikipedia.org/wiki/ICloud_leaks_of_celebrity_photos.

4 « The biggest privacy outrages in 2014 » (Les pires scandales liés à la vie privée de 2014), *Los Angeles Times*, 1er décembre 2014 – http://www.latimes.com/opinion/opinion-la/la-ol-privacy-outrages-of-2014-20141126-story.html.

5 « Bank to trial letting companies target ads at customers based on their payment history » (Une banque compte laisser des entreprises cibler ses clients avec des publicités sur la base de leur historique bancaire), *ZDNet.com*, 11 mars 2014 – http://www.zdnet.com/article/bank-to-trial-letting-companies-target-ads-at-customers-based-on-their-payment-history/.

6 « 'God View': Uber Allegedly Stalked Users For Party-Goers' Viewing Pleasure » (Uber aurait espionné des usagers pour le plaisir de quelques fêtards), *Forbes*, 3 octobre 2014 – http://www.forbes.com/sites/kashmirhill/2014/10/03/god-view-uber-allegedly-stalked-users-for-party-goers-viewing-pleasure/#4ec8d98b3f84.

7 « We Can't Trust Uber » (On ne peut pas avoir confiance en Uber), *New York Times*, 7 décembre 2014 – http://www.nytimes.com/2014/12/08/opinion/we-cant-trust-uber.html.

8 « Fitbit Data Now Being Used In The Courtroom » (Les données générées par les Fitbits sont maintenant utilisées au tribunal), *Forbes*, paru le 16 novembre 2014 – http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/.

9 « Axa et Withings, assurance santé et objet connecté », *web des Objets*, 3 juin 2014 – http://webdesobjets.fr/axa-withings-assurance-sante-objet-connecte/.

10 « Les smartphones et leurs apps sous le microscope de la CNIL et d'Inria », lettre *Innovation et prospective* de la CNIL Nº 8, novembre 2014 – https://www.cnil.fr/sites/default/files/typo/document/Lettre_IP_N-8-Mobilitics.pdf.

11 « Qui d'Apple ou Google saura quand vous faites l'amour ? », *Numerama*, 6 janvier 2015 – http://www.numerama.com/magazine/31782-qui-d-apple-ou-google-saura-quand-vous-faites-l-amour.html.

12 Issu de la page « À propos de Google » : https://www.google.com/about/company/.

13 D'après le *Blog du modérateur*, la part de marché de Google en France en 2015 est de 95,46 %. Le second moteur, Bing, est seulement à 2,2 %. Source : http://www.blogdumoderateur.com/chiffres-google/.

14 « Aux États-Unis, Google dénonce un pédophile qui utilisait Gmail », Aude Deraedt, *Libération*, 5 août 2014 – http://www.liberation.fr/ecrans/2014/08/05/aux-etats-unis-google-denonce-un-pedophile-qui-utilisait-gmail_1075775.

15 http://www.google.fr/intl/fr/policies/terms/regional.html.

16 « Google Engineer Stalked Teens, Spied on Chats (Updated) » (Un ingénieur de Google harcelait les adolescents qu'il espionnait sur le chat), *Gawker*, 14 septembre 2010 – http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats.

17 « Google Confirms That It Fired Engineer For Breaking Internal Privacy Policies » (Google confirme qu'il a déjà licencié un ingénieur pour avoir enfreint les règles relatives à la vie privée), *TechCrunch*, 14 septembre 2010 – http://techcrunch.com/2010/09/14/google-engineer-spying-fired/.

18 « Blackmailer hacks ECB website, steals email addresses and contact details » (Un maître-chanteur pénètre dans le site de la BCE, vole des données personnelles, adresses postales et email), *CityAM*, 24 juillet 2014 – http://www.cityam.com/1406190300/ecb-website-hacked.

19 « Après son piratage, la base de données de Domino's Pizza publiée sur Internet », *Le Monde*, 21 novembre 2014 – http://www.lemonde.fr/pixels/article/2014/11/21/apres-son-piratage-la-base-de-donnee-de-domino-s-pizza-publiee-sur-internet_4525393_4408996.html.

20 « "Unprecedented" cyberattack no excuse for Sony breach, pros say » (Selon les professionnels, l'ampleur de l'attaque n'excuse pas Sony pour ses failles informatiques), *ArsTechnica*, 9 décembre 2014 – http://arstechnica.com/security/2014/12/unprecedented-cyberattack-no-excuse-for-sony-breach-pros-say/.

21 « Experimental evidence of massive-scale emotional contagion through social networks » (Preuve expérimentale d'une contagion émotionnelle à grande échelle par les réseaux sociaux), Adam D. I. Kramera, Jamie E. Guillory et Jeffrey T. Hancock *Proceedings of the National Academy of Sciences of the USA* volume XI, num 24, 25 mars 2014 – http://www.pnas.org/content/111/24/8788.full.

22 « A 61-million-person experiment in social influence and political mobilization » (Une expérience portant sur 61 millions de personnes dans le domaine de l'influence sociale et la mobilisation politique), *Nature*, 2 septembre 2012 – http://www.nature.com/nature/journal/v489/n7415/full/nature11421.html.

23 « Facebook experiment boosts US voter turnout » (Une expérience de Facebook stimule la participation à un vote aux États-Unis), *Nature* – http://www.nature.com/news/facebook-experiment-boosts-us-voter-turnout-1.11401.

24 « Facebook Could Decide an Election Without Anyone Ever Finding Out » (Facebook pourrait influencer une élection sans que personne ne le sache jamais), Jonathan Zittrain, *The New Republic*, 2 juin 2014 – https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering.

25 « Echelon est un nom de code utilisé pendant de nombreuses années par les services de renseignements des États-Unis pour désigner une base d'interception des satellites de télécommunications commerciaux. Par extension, le réseau Echelon désigne le système mondial d'interception des communications privées et publiques (SIGINT), élaboré par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande dans le cadre du traité UKUSA. » Article *Echelon*, sur Wikipédia – https://fr.wikipedia.org/wiki/Echelon.

26 *Nulle part où se cacher*, Glenn Greenwald, JCLattès, mai 2014.

27 *Citizenfour*, Laura Poitras, disponible en DVD.

28 « How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did » (Comment les supermarchés Target ont compris qu'une adolescente était enceinte avant que son père ne l'apprenne), *Forbes*, 16 février 2012 – http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

29 https://www.facebook.com/data/notes.

30 « The Formation of Love » (La formation de l'amour), publié le 14 février 2014 (St Valentin !) sur Facebook – https://www.facebook.com/notes/facebook-data-science/the-formation-of-love/10152064609253859.

31 Photographie intérieure d'un bâtiment d'une prison à Presidio Modelo, Cuba, par Friman – licence Creative Commons –

https://commons.wikimedia.org/wiki/File:Presidio-modelo2.JPG.

32 Glen Greenwald, « Why privacy matters » (En quoi la vie privée est importante) *Conférence TEDGlobal*, octobre 2014, trad. Tristan Nitot – http://www.ted.com/talks/glenn_greenwald_why_privacy_matters/transcript?language=en.

33 Bruce Schneier, « The value of privacy » (La valeur de la vie privée), le 19 mai 2006, trad. Tristan Nitot – https://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html.

34 La création du Tribunal Pénal International, cinquante ans après, est la première tentative de doter ce texte d'un outil de réalisation.

35 Déclaration commune des autorités européennes de protection des données réunies au sein du groupe de l'article 29, datée du 25 novembre 2014 – http://www.cnil.fr/linstitution/international/g29/edgf14/.

36 « The Right to Privacy » (Le droit à la vie privée), Samuel D. Warren et Louis D. Brandeis, *Harvard Law Review*, vol. IV, nº 5, 15, décembre 1890 – http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

37 https://en.wikipedia.org/wiki/Katz_v._United_States.

38 « Il est trop tard pour le Parti Pirate », *L'Obs*, 8 décembre 2014 – http://o.nouvelobs.com/high-tech/20141208.OBS7281/il-est-trop-tard-pour-le-parti-pirate.html.

39 La vidéo, ironiquement, est hébergée chez YouTube, filiale de Google : « Google CEO Eric Schmidt on privacy » (Eric Schmidt, PDG de Google, à propos de la vie privée) – https://www.youtube.com/watch?v=A6e7wfDHzew.

40 « Facebook's Zuckerberg says the age of privacy is over » (Zuckerberg, de Facebook, dit que la période où on avait une vie privée est terminée), *ReadWrite*, 9 janvier 2010 – http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov/.

41 « Mark Zuckerberg buys four houses near his Palo Alto home » (Mark Zuckerberg achète quatre maisons autour de son domicile de Palo Alto), *Mercury News*, 11 octobre 2013 – http://www.mercurynews.com/business/ci_24285169/mark-zuckerberg-buys-four-houses-near-his-palo-alto-home.

42 « Google's Eric Schmidt Spent $15 million On A NYC Penthouse, And Then Made It Soundproof » (Eric Schmidt de Google dépense 15 millions de dollars pour un duplex avec terrasse au sommet d'un immeuble de New York), *Business Insider*, 25 juillet 2013 – http://www.businessinsider.com/eric-schmidt-spent-15-million-on-a-new-york-penthouse-2013-7.

43 « Inside Google Chairman Eric Schmidt's lavish sex palace » (Dans le somptueux lupanar d'Eric Schmidt, président de Google), *New York Magazine*, 25 juillet 2013 – http://nymag.com/daily/intelligencer/2013/07/eric-schimdt-penthouse-new-york-photos-apartment.html.

44 « Google CEO says privacy doesn't matter. Google blacklists CNet for violating CEO's privacy » (Le PDG de Google explique que la vie privée n'a pas d'importance. Mais Google met CNet sur liste noire pour avoir dévoilé des éléments de la vie privée de son PDG), *BoingBoing*, 9 décembre 2009 – http://boingboing.net/2009/12/09/google-ceo-says-priv.html.

45 BLARNEY, un des programmes de surveillance des communications de la NSA. Détails sur https://en.wikipedia.org/wiki/Blarney_%28code_name%29 et https://www.nsa-observer.net/category/program/family/collect/name/BLARNEY.

46 « Nom mer le conflit. Le cas de l'Alsace pendant son annexion de fait au Troisième Reich, 1940-1945 », Anne-Ségolène Verneret, *Trajectoires*, nº 5, 2011 – https://trajectoires.revues.org/828.

47 « Après l'assignation à résidence, l'humiliation continue », Pierre Alonso, *Libération*, 12 mai 2016 – http://www.liberation.fr/france/2016/05/12/apres-l-assignation-a-residence-l-humiliation-continue_1452147.

48 « État d'urgence : l'État condamné pour une assignation à résidence », *Le Point*, 22 janvier 2016 – http://www.lepoint.fr/societe/etat-d-urgence-l-etat-condamne-pour-une-assignation-a-residence-22-01-2016-2011990_23.php.

Partie II

Au royaume d'internet, le code, c'est la loi

Les mécanismes de la surveillance

Partie II
Au royaume d’internet, le code, c’est la loi

Les mécanismes de la surveillance

10. Contrôler pour ne pas être contrôlé

Comme nous l'avons vu depuis le début de cet ouvrage, la situation en termes de contrôle de la vie privée n'est guère rassurante. Nos données sont collectées par des grands services souvent américains, par notre équipement, du PC au smartphone, avec de nouveaux capteurs comme les *trackers* d'activité physique. « L'internet des objets », composé par les nouveaux objets dits intelligents, du détecteur de fumée aux thermostats intelligents, ne va faire qu'enfoncer le clou.

Par ailleurs, les services secrets de certains pays peuvent se brancher directement sur notre équipement ou vont plus simplement espionner les grands services commerciaux qui savent tout de nous. Même si le respect de la vie privée est inscrit dans la loi, chacun peut constater que la notion s'érode, sous les coups de boutoir des médias sociaux d'un côté, et de la volonté des politiques et des services de renseignements de contrôler internet, de l'autre.

Pourtant, nous sommes chaque jour un peu plus dépendants de l'informatique. Aussi, la question n'est pas d'arrêter de se servir de l'informatique mais de comprendre comment elle fonctionne, de façon à savoir comment la contrôler et surtout contrôler l'usage qui est fait de nos données. Car c'est bien là l'enjeu du futur : contrôler l'outil informatique pour éviter qu'il ne nous contrôle ou permette à d'autres de nous contrôler.

11. Que peut-on contrôler ?

Sans le savoir, à chaque fois que nous utilisons un PC, une tablette, un smartphone ou même tout système informatique, nous manipulons à la fois des données, du matériel et du logiciel. Quelques explications s'imposent pour bien comprendre comment il est possible de conserver le contrôle de l'outil informatique. Que les puristes me pardonnent d'enfoncer des portes qui leur sont déjà ouvertes !

Le matériel est facile à identifier : c'est ce qui est tangible et peut prendre la forme d'un smartphone, d'un PC de bureau (une unité centrale avec un clavier, un écran et une souris), d'une tablette ou d'un ordinateur portable. On peut diviser conceptuellement le matériel en trois parties : l'unité centrale qui est « le cerveau » de l'ordinateur traitant les données, les périphériques qui lui permettent de récupérer et d'échanger de l'information (écran, clavier, souris, écran tactile, divers capteurs, interface réseau avec ou sans fil) et enfin la mémoire de masse, pour y stocker les données (disque dur, carte mémoire).

Le logiciel est pour sa part immatériel, c'est-à-dire qu'on ne peut pas le toucher. Ça peut être un système d'exploitation (Windows, OSX, iOS, Android, GNU/Linux) ou une application (Word, Excel, LibreOffice, Mozilla Firefox, VLC, Gmail, Spotify, etc.). Pour simplifier, un logiciel est une suite ordonnée d'instructions (le code) que l'on donne au matériel pour lui indiquer comment manipuler les données. Le code décrit le processus de manipulation des données.

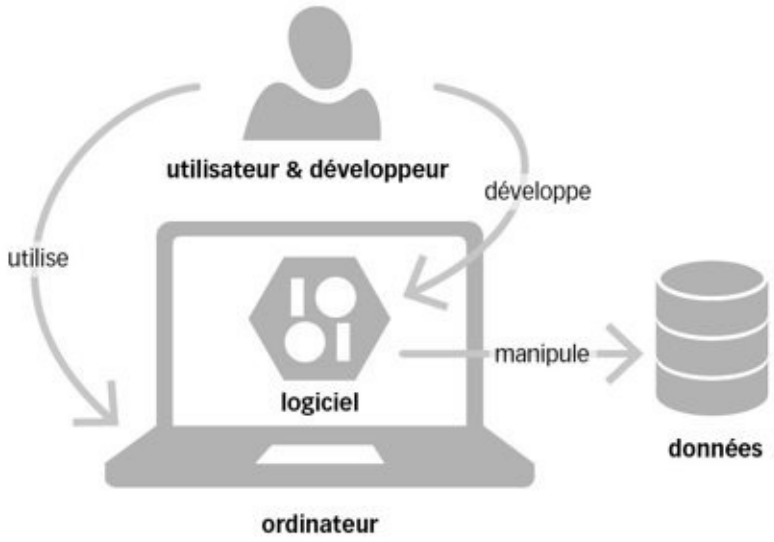
Les données, toujours pour simplifier, ce sont des informations. Une liste de noms et de numéros de téléphone qu'on stockera dans un smartphone ; les montants des ventes saisis dans Excel pour faire des calculs ; une chanson numérisée ; une photo numérique qu'on retouchera avec un logiciel adapté. Les données sont souvent ce qui est le plus important pour l'utilisateur car elles lui sont souvent spécifiques.

Les trois parties du système sont indissociables : sans matériel, le logiciel ne sert à rien et l'on ne peut pas traiter les données. Sans les instructions du logiciel, la puissance de traitement du matériel ne peut pas être utilisée pour traiter les données.

12. Contrôle et informatique personnelle

À la fin des années soixante-dix, au tout début de la micro-informatique, la problématique du contrôle de l'informatique était toute simple : les premiers micro-ordinateurs étaient livrés quasiment sans logiciels et n'étaient pas connectés à internet. Comme ils étaient destinés à des hobbyistes, des électroniciens et des bidouilleurs, l'utilisateur devait apprendre à écrire le logiciel dont il avait besoin.

C'était la situation idéale en termes de contrôle de l'informatique : l'utilisateur saisissait lui-même ses données dans un logiciel dont il avait pleinement le contrôle, puisqu'il l'avait écrit, sur un ordinateur qui était physiquement devant lui.



éééé

Schéma décrivant les échanges et les rapports entre un ordinateur, un logiciel, les données et un utilisateur ou développeur, sous forme de cycle.

On le verra, cette situation idéale d'un contrôle total par l'utilisateur ne durera pas.

Dans la grande confrérie des développeurs amateurs des premiers micro-ordinateurs, le partage était la norme : devant la rareté des logiciels disponibles, il était normal de partager les logiciels qu'on avait écrits avec d'autres hobbyistes. Le logiciel qu'on venait de recevoir ne fonctionnait pas exactement comme on voulait ? Qu'à cela ne tienne, il suffisait de le modifier pour corriger le problème. Pour cela, il faut comprendre comment fonctionne le logiciel, ce qui est possible s'il est relativement simple et écrit de façon structurée par son auteur.

Mais au fur et à mesure que la micro-informatique est devenue une industrie, que les utilisateurs ont compris le potentiel de l'informatique, que les besoins sont devenus plus complexes avec des enjeux plus importants, certains utilisateurs avancés sont devenus des développeurs de logiciels professionnels à temps plein.

Ce changement, cette professionnalisation, bienvenue pour régler le problème de la complexité croissante des besoins et des logiciels, a créé un nouveau problème : tandis que jusqu'alors le

développeur et l'utilisateur étaient la même personne et avaient donc des intérêts communs, on se retrouve alors avec un utilisateur qui veut un logiciel répondant à ses besoins propres, quand le développeur cherche au contraire à écrire une seule fois un logiciel qui réponde aux besoins du plus grand nombre, pour pouvoir le vendre au maximum de clients possibles et ainsi rentabiliser au mieux son investissement en développement.

Le développeur de logiciels est dans les faits devenu un « éditeur d'applications » ou un « prestataire de services », et l'utilisateur dispose de logiciels créés par un tiers : l'utilisateur dépend dorénavant du bon vouloir du développeur.

13. Le code, c’est la loi

Il y a dans l’histoire de l’informatique un événement d’apparence anodine qui a eu une grande importance : le jour où Richard Stallman a rencontré un problème avec la nouvelle imprimante de son bureau.

En 1980, Richard Stallman est informaticien et chercheur au laboratoire d’intelligence artificielle du MIT (Massachusetts Institute of Technology), célèbre université américaine. Le laboratoire vient de recevoir une imprimante très perfectionnée dont le logiciel comporte, comme tout logiciel, des imperfections, des bogues. Richard Stallman contacte le fabricant de l’imprimante et demande le code source du logiciel en vue de le corriger. Le fabricant le lui refuse. Pour eux, le logiciel est « propriétaire », son contenu doit donc rester secret pour éviter que des concurrents ne le copient et l’améliorent.

Pour rester le plus clair possible, nous devons distinguer code source et code binaire. Dans la plupart des cas, un logiciel existe sous ces deux formes : le code source, lisible et compréhensible par les informaticiens, et le code binaire, compréhensible uniquement par la machine. La transformation du code source en code binaire s’appelle la compilation. Il est quasiment impossible pour un humain de comprendre le code binaire : en conséquence, les modifications du logiciel ne se font que sur le code source (sauf très rares exceptions). Les entreprises qui veulent rester « propriétaires » de leurs logiciels ont tendance à distribuer leurs logiciels uniquement sous code binaire, rendant ainsi les utilisateurs, même les plus avancés et compétents en informatique, dépendants des personnes qui ont accès au code source.

Richard Stallman, venant du monde universitaire où le partage du code source et la collaboration entre informaticiens étaient la norme, a considéré cette situation comme moralement inacceptable : elle limite la liberté des utilisateurs et les rend directement dépendants des éditeurs de logiciels. Par ailleurs, ces derniers font signer aux utilisateurs de leurs logiciels des contrats de licence qui leur interdisent de les modifier et de les redistribuer. Ce sont ces contrats que l’on accepte trop souvent sans les lire, simplement en cliquant sur « installer » ou en acceptant les « conditions générales d’utilisation » quand on télécharge un logiciel sur son ordinateur ou sur un appareil mobile. Pour Richard Stallman, interdire la collaboration et le partage est mauvais pour la société et néfaste pour le progrès technologique.

Pour contrer cela, Richard Stallman, qui a de la suite dans les idées, fonde le projet GNU. Il invente le concept de logiciel libre et crée la licence GNU *General Public License* (GNU GPL), le contrat de licence le plus utilisé au monde pour diffuser des logiciels libres.

Voici la définition par Richard Stallman d’un logiciel libre [49] :

Un programme est un logiciel libre pour vous, utilisateur particulier, si :

- vous avez la liberté de l’exécuter comme vous le voulez, pour quelque motif que ce soit ;
- vous avez la liberté de modifier le programme afin qu’il corresponde mieux à vos besoins (dans

la pratique, pour que cette liberté prenne effet, il vous faut pouvoir accéder au code source, puisque opérer des modifications au sein d'un programme dont on n'a pas le code source est un exercice extrêmement difficile) ;

vous disposez de la liberté d'en redistribuer des copies, que ce soit de manière gratuite ou onéreuse ;

vous avez la liberté de distribuer des versions modifiées du programme, afin que la communauté puisse bénéficier de vos améliorations.

Le projet GNU, lui aussi initié par Richard Stallman, vise à créer un système d'exploitation (logiciel de base permettant de faire tourner des applications) qui soit entièrement libre. Aujourd'hui, le projet GNU est surtout connu pour le logiciel GNU/Linux, souvent appelé en résumé Linux, utilisé par des centaines de millions de gens dans des smartphones, des « box » ADSL, des ordinateurs de bureau, des serveurs (dont ceux de Google et Facebook), et par l'essentiel de l'infrastructure d'internet (gestion du réseau et des serveurs web).

Richard Stallman a clairement mis en évidence que celui qui écrit le programme dispose d'un ascendant énorme, et peut décider à la place de l'utilisateur ce que celui-ci peut faire ou ne pas faire. Avec la notion de logiciel libre, c'est finalement l'utilisateur du logiciel qui devient libre, bien plus que le logiciel en tant que tel.

La contribution de Lawrence Lessig

En 1999, dans un livre appelé *Code and other laws of Cyberspace*, le juriste américain Lawrence Lessig explique comment, dans notre société informatisée, le code informatique a donné le pouvoir aux développeurs aux dépens des utilisateurs. Lessig démontre qu'il fut un temps où la loi décidait ce que le citoyen avait le droit de faire ou non, mais ce rôle est de plus en plus souvent joué par un logiciel ou un service, par du code informatique. On peut le constater quand un logiciel nous interdit de faire ce que l'on veut : à moins qu'il ne soit libre et donc que son code soit librement modifiable, l'utilisateur est à la merci du développeur qui a écrit le logiciel.

En ce qui concerne la loi, son écriture et son adoption se font dans le cadre d'un processus démocratique, avec des amendements, des débats contradictoires entre juristes, avant d'être votée par des représentants des citoyens. À l'inverse, le logiciel est souvent écrit par une société commerciale dont les intérêts sont de fidéliser les clients, et il n'y a rien de plus fidèle qu'un client qui ne peut pas partir parce qu'on l'en empêche, par exemple en rendant compliquée l'exportation de ses données vers des solutions concurrentes.

Un utilisateur choisit un logiciel pour répondre à un besoin mais sans comprendre son fonctionnement interne, ni s'interroger sur la possibilité de récupérer ses données s'il choisit plus tard une autre solution.

En plus de la liberté, la transparence

Il existe un autre avantage au logiciel libre : le fait que l'on puisse lire son code source le rend (relativement) transparent. En effet, nous avons vu que le code source d'un logiciel propriétaire n'est pas visible. Il est ainsi possible que ce logiciel nuise, directement ou indirectement, à l'utilisateur ou à

sa sécurité sans que ce dernier ne s'en rende compte. En utilisant un logiciel propriétaire, nous sommes face à une « boîte noire » que nous ne contrôlons pas.

Cela a donné lieu à de nombreuses controverses, où plusieurs logiciels très répandus 50 comme Microsoft Windows 51, la messagerie Lotus Notes 52 ou Skype 53 pourraient avoir des portes dérobées permettant à des espions de la NSA (espionnage informatique américain) d'accéder facilement aux données des utilisateurs. Le code de ces produits est opaque, il ne peut être audité facilement. Il est donc quasiment impossible de savoir si de telles portes dérobées ont bien été créées volontairement par les développeurs à la demande des services secrets américains ou non.

Ce débat existe également en dehors du réseau, pour des logiciels embarqués dans des produits courants. L'affaire Volkswagen en est un exemple : parce que nul ne pouvait vérifier ce que faisait le logiciel, les ingénieurs ont pu truquer le rendement des voitures pour respecter les normes de pollution lors des contrôles techniques… mais pas dans les usages quotidiens. Le code fermé est dangereux pour toute la société 54.

Le logiciel libre, parce que son code source est lisible, est exposé au regard permanent de programmeurs ou d'experts en sécurité et son fonctionnement examiné dans le détail. Au-delà de la liberté de faire ce que l'on veut et au-delà du contrôle de ce que fait le logiciel, cette transparence nous permet d'avoir confiance dans le logiciel libre en question, même s'il est écrit par d'autres.

14. Internet change la donne

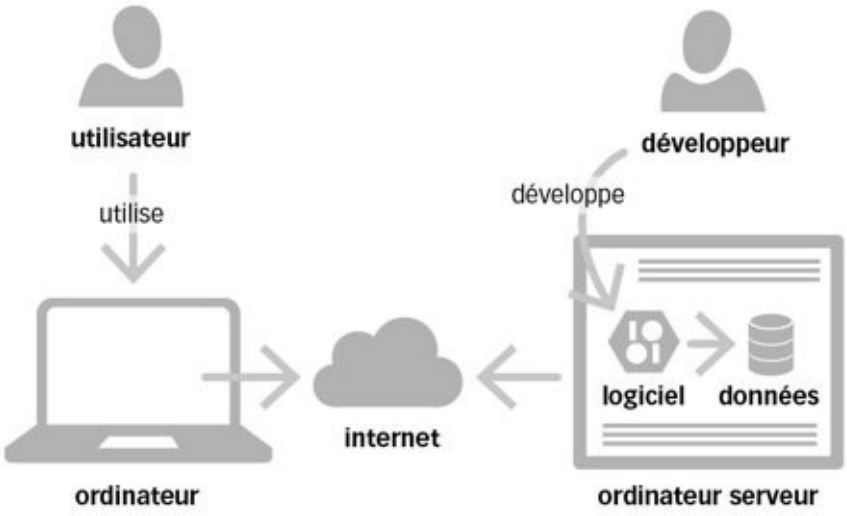
Nous sommes aujourd'hui bien loin de la micro-informatique des années quatre-vingt. Les ordinateurs ont été miniaturisés au point qu'on peut en avoir un dans la poche (un smartphone) ou dans un sac à main (une tablette) ou dans un cartable (un ordinateur portable).

On oublie souvent à quel point les choses ont progressé ces quatre dernières décennies. Voici deux exemples :

l'iPad 2 est aussi puissant qu'un Cray 2 (supercalculateur) de 1985 55.

Chacune de nos recherches sur le moteur Google utilise la puissance de calcul équivalente à celle utilisée par le programme spatial Apollo dans les années soixante 56.

Au-delà de cette miniaturisation et de ce gain de puissance, l'informatique a changé de nature dans la mesure où il est devenu très rare d'utiliser un ordinateur qui ne soit pas connecté à d'autres ordinateurs via un réseau (un réseau est ce qui permet de connecter un ordinateur à d'autres pour échanger de données. Cette connexion peut se faire par un fil mais aussi par ondes radio, le plus souvent par la norme wifi).



éé

Schéma décrivant le concept de logiciel comme service, avec les rapports entre l'ordinateur, l'utilisateur, et les logiciels et les données hébergés sur d'autres ordinateurs via internet.

Via le réseau, on se retrouve à utiliser des ordinateurs à distance. Ainsi, quand on fait une recherche Google sur un mot-clé, on fait un appel à des ordinateurs situés dans un centre de données (data center), une sorte de hangar climatisé où se trouvent des centaines d'ordinateurs (les serveurs) qui reçoivent les recherches des utilisateurs et renvoient des résultats. Notre ordinateur (ou notre tablette ou smartphone) ne fait qu'afficher les résultats de notre demande.

Quel contrôle sur nos données et nos ordinateurs avons-nous à l'heure d'internet ?

Prenons un peu de recul un court instant et revenons-en aux premiers pas de la micro-informatique.

Au début, l'utilisateur avait le contrôle des logiciels utilisés, car il avait dû les écrire lui-même, à moins qu'il n'ait récupéré du code source venant d'un autre hobbyiste. Ses données étaient stockées localement, donc l'utilisateur en avait également le contrôle.

Si nous revenons à l'époque présente, correspondant au schéma ci-dessus, on peut certes faire plus de choses qu'avant, et c'est tant mieux, mais en termes de contrôle de nos logiciels et nos données c'est la descente aux enfers… Dorénavant, le logiciel qui tourne sur nos ordinateurs est presque toujours propriétaire, c'est-à-dire écrit par un tiers et dont le fonctionnement est quasiment invérifiable. Comment avoir confiance dans ces boîtes noires ? Mais il y a pire : nos PC nous servent surtout à utiliser du logiciel qui fonctionne en fait sur des serveurs, lesquels sont dans des data centers distants. Là aussi il s'agit le plus souvent d'applications propriétaires, écrites par des tiers. Et le comble, c'est que nos données sont là-bas, dans ces mêmes data centers !

C'est une totale aberration : l'informatique est chaque jour plus indispensable à nos vies, et pourtant nous perdons chaque jour des capacités de contrôle !

Auparavant, les ordinateurs nous appartenaient, utilisaient du logiciel que nous pouvions auditer et modifier, et nos données étaient stockées localement.

Maintenant, les ordinateurs sont dans des data centers dont on ignore jusqu'à la localisation, avec des logiciels écrits par d'autres et qu'on ne peut pas auditer, et nos données sont détenues par des tiers ! Ces mêmes tiers en profitent pour accumuler des données sur la façon dont nous utilisons ces logiciels, mais possèdent aussi nos propres données…

Quand je pense à ça, je me dis que le monde marche sur la tête.

Revenons sur l'impossibilité de savoir ce qui est fait de nos données. Quelles informations personnelles sont collectées ? Quelles informations à propos de mes proches sont récupérées via mes échanges avec eux ? Combien de temps sont-elles conservées ? Avec qui sont-elles partagées ? Comment sont-elles recoupées ?

Nous n'avons aucun contrôle sur les logiciels qui tournent sur les machines des services internet auxquels nous avons recours. Sans aucune possibilité de contrôle, comment peut-on avoir confiance ? Il ne nous reste plus qu'à nous fier aux promesses des services que nous utilisons, sans avoir les moyens de savoir si elles seront tenues.

Pire : quand on analyse ces promesses, telles qu'elles sont contenues dans des documents appelés « politiques d'utilisation des données » ou « règles de confidentialité » (*privacy policies* en anglais), on se rend compte que tout cela est incompréhensible pour l'utilisateur ordinaire car trop long et écrit dans un langage qui mêle la complexité technique à la complexité juridique.

Je vous propose de voir ce que Facebook et Google, à titre d'exemple, annoncent faire de nos données. Ça n'est guère rassurant…

Quelles données sont collectées par Facebook ?

Prenons la politique d'utilisation des données de Facebook [57]. Il suffit de passer un peu de temps à

analyser ces documents pour voir que « *pour fournir un meilleur service* », l'entreprise collecte des données, beaucoup de données, toutes sortes de données. Extrait du document de Facebook :

Nous utilisons les informations que nous recevons pour les services et les fonctions que nous vous fournissons, à vous et à d'autres utilisateurs, tels que vos amis, nos partenaires, les annonceurs qui achètent des publicités sur le site.

Quelles informations 58, plus précisément ?

> informations d'inscription ;
>
> informations que vous choisissez de communiquer ;
>
> informations que d'autres communiquent à votre propos ;
>
> autres informations que nous recevons à votre sujet.

Cette dernière section du document Facebook est particulièrement intéressante, parce que nous n'en n'avons que rarement conscience : de nombreuses données sont collectées sur notre comportement, sans que nous ne les partagions sciemment avec ce service. Quelques extraits :

> Nous recevons également d'autres types d'informations vous concernant :
>
> nous recevons des données à votre sujet à chaque fois que vous entreprenez une action dans Facebook […] ;
>
> lorsque vous publiez des informations telles que des photos ou des vidéos sur Facebook, nous pouvons recevoir des données supplémentaires (ou métadonnées), comme l'heure, la date et l'endroit où vous avez pris la photo ou la vidéo ;
>
> nous recevons des données provenant de, ou concernant, l'ordinateur, le téléphone mobile ou les autres équipements dont vous vous servez pour installer les applications Facebook ou pour accéder à Facebook […]. Cela peut comprendre des informations sur […] le type (y compris les numéros d'identification) de l'appareil ou du navigateur que vous utilisez ou les pages que vous visitez. Par exemple, nous pouvons obtenir vos coordonnées GPS ou d'autres informations de géolocalisation […] Nous recueillons également les données provenant d'informations que nous possédons déjà à votre sujet et à propos de vos amis et de tiers […] Nous pouvons associer votre ville actuelle, vos coordonnées GPS […] ;

Quelles données sont collectées par Google ?

En ce qui concerne Google, même si le type de service rendu est différent, la collecte de données est elle aussi généralisée. Il faut dire que la mission que s'est choisie l'entreprise est « *(d')organiser l'information du monde, de la rendre utile et accessible de partout* ». Et pour cela, il lui faut collecter toutes les données possibles, comme nous l'avons vu au chapitre 3.

Passons donc en revue les règles de confidentialité de Google 59 :

Au-delà des données que nous communiquons volontairement à Google, la société collecte :

> […] des données relatives à l'appareil que vous utilisez, par exemple, le modèle, la version du système d'exploitation, les identifiants uniques de l'appareil et les informations relatives au réseau mobile, y compris votre numéro de téléphone. […] ;

la façon dont vous avez utilisé le service concerné, telles que vos requêtes de recherche ;

des données relatives aux communications téléphoniques, comme votre numéro de téléphone, celui de l'appelant, les numéros de transfert, l'heure et la date des appels, leur durée, les données de routage des SMS et les types d'appels ;

votre adresse IP ;

des données relatives aux événements liés à l'appareil que vous utilisez, tels que plantages, activité du système, paramètres du matériel, type et langue de votre navigateur, date et heure de la requête et URL de provenance ;

[…] nous utilisons différentes technologies pour vous localiser, y compris l'adresse IP, les signaux GPS et d'autres capteurs nous permettant notamment d'identifier les appareils, les points d'accès wifi et les antennes-relais se trouvant à proximité ;

[nous] utilisons les informations fournies par les cookies et d'autres technologies, comme les balises pixel […] ;

nos systèmes automatisés analysent vos contenus (y compris les e-mails) […] ;

les informations personnelles que vous fournissez pour l'un de nos services sont susceptibles d'être recoupées avec celles issues d'autres services Google (y compris des informations personnelles), […]

même lorsque vous supprimez des données utilisées par nos services, nous ne supprimons pas immédiatement les copies résiduelles se trouvant sur nos serveurs actifs ni celles stockées dans nos systèmes de sauvegarde.

J'ai décidé de me limiter aux aspects les plus frappants de deux des acteurs les plus utilisés, mais il faut savoir deux choses : la plupart des services en ligne (mais pas tous, heureusement) ont des conditions d'utilisation qui sont comparables ; en les utilisant, nous acceptons par défaut ces conditions d'utilisation et reconnaissons les avoir lues.

Voyons voir pourquoi la plupart des services en ligne sont aussi voraces dès qu'il s'agit de nos données personnelles…

15. Le piège de la gratuité

Il y a un grand, un immense malentendu quant aux grands services commerciaux du genre Facebook, Google, Twitter et tous les services dits « gratuits ». On entend d'ailleurs souvent l'adage suivant : « *Si c'est gratuit, c'est vous le produit.* »

En effet, si un tel service est gratuit, vous n'êtes pas le client. Le client, par définition, c'est celui qui paye.

Mais qui est le client, alors ?

Si un service commercial, coté en Bourse où il est valorisé à plusieurs milliards de dollars, est gratuit, il y a bien quelqu'un qui paye. Ce sont ceux qui payent qui méritent d'être appelé les clients.

Les revenus des entreprises de technologie se partagent entre les revenus boursiers et les revenus publicitaires. Le premier client est l'investisseur, qu'il faut choyer en lui promettant des dividendes à venir… dans notre cas, des dividendes garantis par l'accumulation de données personnelles qui forment un « actif immatériel » de l'entreprise, qui pourra être revendu sur le marché des entreprises.

Mais c'est l'annonceur publicitaire qui fournit actuellement le gros des revenus. C'est lui qui paye le service que vous utilisez. Pourquoi ? Pour pouvoir avant tout mettre de la publicité dans le service. Vous me rétorquerez que c'est comme quand on regarde la télévision, payée en partie par la redevance TV (un genre d'impôt) et en partie ou en totalité par la publicité. Cela avait en particulier poussé l'ancien patron de TF1, Patrick Le Lay, à déclarer 60 :

« À la base, le métier de TF1, c'est d'aider Coca-Cola, par exemple, à vendre son produit. […] Or pour qu'un message publicitaire soit perçu, il faut que le cerveau du téléspectateur soit disponible. Nos émissions ont pour vocation de le rendre disponible : c'est-à-dire de le divertir, de le détendre pour le préparer entre deux messages. Ce que nous [TF1] vendons à Coca-Cola, c'est du temps de cerveau humain disponible. »

Voilà, ce que vendent les grands services en ligne, c'est « du temps de cerveau humain disponible », mais c'est aussi bien plus que ça : ils vendent aux annonceurs de la publicité dite « ciblée », c'est-à-dire de la publicité qui est censée correspondre aux centres d'intérêt des utilisateurs. Plus ces grands services connaissent leurs utilisateurs, plus ils sont capables d'afficher ce que l'utilisateur peut avoir envie d'acheter. Un ciblage personnalisé que les annonceurs sont prêts à payer beaucoup plus.

Il ressort de cela deux choses essentielles à bien comprendre pour saisir comment fonctionne l'essentiel de la partie commerciale d'internet : plus les services en question en savent sur nous, plus notre temps de cerveau disponible est facturé cher aux annonceurs.

Et aussi : quand nous utilisons Google ou Facebook, nous laissons nos données personnelles en échange d'un service.

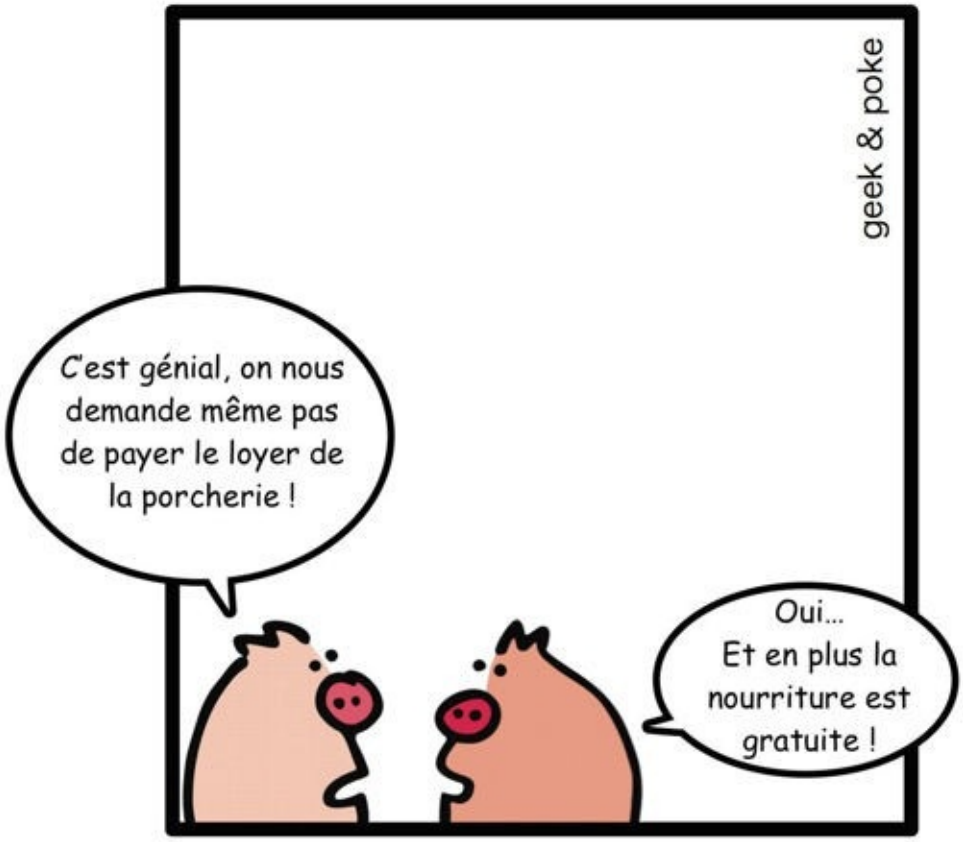
En échange de quelques verroteries

Cet échange est-il une bonne affaire ? Ne serait-ce pas plutôt un marché de dupes ?

D’un côté, il faut déterminer combien valent nos données personnelles. C’est difficile à dire, mais si on considère que la vie privée est protégée par plusieurs lois (cf. chapitre 8) parce qu’elle est indispensable à notre liberté, on peut estimer qu’elle vaut beaucoup, comme notre liberté elle-même.

À l’inverse, contre quoi échangeons-nous ces données personnelles ? Un service. Combien coûte ce service ? Prenons le cas de Facebook pour faire un rapide calcul qui se révèle très instructif. Facebook a des dépenses opérationnelles annuelles de 6,225 milliards de dollars [61] pour 1,591 milliard d’utilisateurs [62] ? Un rapide produit en croix nous donne ce constat affligeant : chaque utilisateur de Facebook échange ses données personnelles contre un service coûtant 3,91 $ (soit 3,33 €) par an.

Je vais laisser la conclusion de ce chapitre à Geek & Poke :


geek & poke
C'est génial, on nous demande même pas de payer le loyer de la porcherie !
Oui... Et en plus la nourriture est gratuite !
Deux cochons discutant du modèle « gratuit »

è

Deux cochons discutant du modèle « gratuit » (geek & poke, licence CC-by) [63].

Deux cochons discutant du modèle « gratuit ». Le premier personnage : « C'est génial, on ne nous demande même pas de payer le loyer de la porcherie ! ». Le second cochon : « Oui... Et en plus la nourriture est gratuite. »

Comme les deux cochons ci-dessus discutant du modèle gratuit, acceptons-nous de finir en saucisson numérique contre des services gratuits ? Sommes-nous aussi naïfs que ces cochons à croire qu’ils sont clients du fermier ?

16. Le modèle freemium

Il existe une autre catégorie de services en ligne qui utilisent un autre modèle d'affaire que l'on appelle le *freemium*, un concept qui combine gratuité (*free*) et payant haut de gamme (*premium*). En substance, ces services offrent une version gratuite limitée et une version complète plus sophistiquée mais payante. C'est le cas de nombreux services comme Spotify (musique en ligne), Evernote (prise de notes), RememberTheMilk (liste de choses à faire), Dropbox (stockage en ligne).

Quand on écoute les dirigeants des entreprises proposant ces services, on entend dire que les utilisateurs payants financent le service pour tout le monde. Pourtant, rien n'est vraiment clair sur la sécurité des données fournies à ces sociétés. Pire, on découvre parfois que nos données que l'on croyait protégées sur ces serveurs, sont accidentellement visibles par certains 64, que les mots de passe de millions d'utilisateurs semblent se retrouver dans la nature 65. Il arrive aussi qu'un service ferme ses portes faute de rentabilité ou décide de virer un utilisateur 66, qui perd ainsi toutes ses données et ses contacts 67.

Certains services *freemium* semblent dignes de confiance si l'on en croit leurs conditions générales d'utilisation, mais ça n'est jamais simple. Evernote est un bon exemple : ce service affirme « *vos données n'appartiennent qu'à vous, (et elles) sont protégées* », mais les conditions d'utilisation 68 et les multiples documents afférents sont bien trop longs (79 pages A4 !) et complexes pour que l'utilisateur puisse en être certain.

Payer mais être espionné tout de même !

Prenons un autre exemple, dans une catégorie d'applications très différente, avec les jeux très populaires que sont *Candy Crush Saga* et *Angry Birds* (ce dernier a été téléchargé plus d'un milliard de fois !) Ces jeux peuvent être téléchargés gratuitement mais rapportent de très grosses sommes d'argent à leurs concepteurs en permettant aux joueurs d'acheter des niveaux supplémentaires ou des façons de tricher pour accéder au niveau supérieur. À ce titre, ces jeux participent du modèle *freemium.*

Pourtant, ces revenus énormes ne semblent pas suffire aux dirigeants et actionnaires de ces sociétés, et il semblerait que la NSA et son homologue anglais GCHQ puissent siphonner nos données personnelles depuis ces applications 69. Rovio, la société qui développe *Angry Birds*, nie transmettre des données à la NSA et à GCHQ mais reconnaît récupérer des données personnelles sur les utilisateurs, dont un identifiant du téléphone (genre de numéro de série), l'âge et le sexe de l'utilisateur ainsi que le lieu où il se trouve. Ils collaborent avec des agences publicitaires pour afficher des publicités dans le jeu, et ces agences compilent pour chaque utilisateur des données dont certaines sont franchement dérangeantes, comme par exemple l'origine ethnique, le statut marital (avec des choix comme « célibataire », « fiancé », « marié », « divorcé » et, pour faire bonne mesure, « partenaires multiples ») et son orientation sexuelle avec des choix comme « hétéro », « homo », « bisexuel », et « incertain ». Rappelons que ces jeux sont très souvent utilisés par des enfants…

Comme nous l’avons vu au chapitre 14, le fait que nous n’avons aucun contrôle sur les logiciels propriétaires que nous utilisons et encore moins sur les serveurs distants qui hébergent les services que nous utilisons nous empêche de savoir la vérité sur ces questions essentielles : sommes-nous observés ? Quelles données sont collectées ? Combien de temps sont-elles gardées ? Comment sont-elles agrégées pour nous profiler ? Que faire si ces profils ont un impact sur notre vie ? Que faire si en plus ces profils sont inexacts ?

Certains services en ligne sont innovants et très utiles. D’autres au contraire sont de véritables sangsues à données. Le problème est qu’il est difficile de faire la différence entre les deux. Une chose est sûre : tout service affichant de la publicité est hautement suspect car il a tout intérêt financièrement à profiler les utilisateurs de façon à vendre aux annonceurs une publicité ciblée donc plus lucrative.

17. Faut-il avoir confiance en Apple ?

Apple est un cas à part dans l'informatique. À la différence de Google et de Facebook qui sont des services en ligne financés par la publicité ciblée, Apple conçoit et commercialise du matériel informatique (smartphones iPhone, tablettes iPad, et les PC MacBook et iMac). Comme ce matériel a de surcroît un positionnement haut de gamme, les marges sont importantes et permettent de financer des services en ligne d'apparence gratuite si vous avez acheté du matériel coûteux. Ce matériel étant renouvelé tous les deux à cinq ans, et le service incitant les utilisateurs à rester chez Apple, la pérennité du service est assurée, d'autant qu'une tarification d'iCloud à la mode *freemium* (5 Go gratuits et facturation de la capacité supplémentaire 70) fait qu'Apple n'a pas besoin d'avoir recours au profilage des utilisateurs à des fins publicitaires.

Cela ne suffit malheureusement pas pour rassurer les clients sur la sécurité de leurs données, et ceci pour plusieurs raisons. En effet, comme tous les logiciels et services, la marque à la pomme a connu quelques incidents côté vie privée.

Les fuites de données des Mac

En 2014, Apple sortait une nouvelle version de son système d'exploitation pour Mac, OSX 10.10 surnommé Yosemite. Celui-ci souhaitait se positionner comme système plus respectueux de la vie privée des utilisateurs car il permet de faire des recherches sur le web avec le moteur DuckDuckGo, un concurrent de Google dont le principal intérêt est de ne pas collecter de données personnelles. Pourtant, des utilisateurs ont remarqué que dans certains cas, des données étaient néanmoins envoyées à Apple 71, même quand le Mac est paramétré pour être dans la configuration la plus « paranoïaque » possible (utilisation de DuckDuckGo, pas d'utilisation du stockage en ligne iCloud d'Apple, etc.).

L'iPhone n'est pas mieux loti

En ce qui concerne l'iPhone, on est en droit d'avoir de sérieux soupçons, car Edward Snowden, le lanceur d'alerte, refuse d'en utiliser un 72 suite aux documents qui expliquent que la NSA peut y accéder à distance, via le programme DROPOUTJEEP 73. Voici un extrait des documents précisant ce qu'il est possible de faire à un iPhone :

(Ce logiciel permet de) lire et écrire des fichiers à distance de/vers le téléphone, récupérer les SMS, retrouver les contacts du carnet d'adresses, la messagerie vocale, la localisation géographique, écouter le micro à la demande, prendre une photo, déterminer quelle tour GSM est utilisée. La prise de contrôle et la récupération des données peut être effectuée via des SMS ou une connexion GPRS. Toutes les communications via ce logiciel implanté seront invisibles et chiffrées.

On notera que la NSA explique à demi-mot que le logiciel n'est pas installé en standard dans l'iPhone mais doit y être « implanté » d'une façon ou d'une autre, sans donner de détails. On peut supposer que cela peut être fait par une application d'apparence inoffensive, un jeu par exemple, selon le principe du cheval de Troie 74.

Le manque de compréhension des utilisateurs

Une partie du problème est le manque d'information et de compréhension des utilisateurs de produits technologiques.

Comme le disait l'écrivain de science-fiction Arthur C. Clarke : « *Toute technologie suffisamment avancée est indiscernable de la magie.* »

C'est une des grandes raisons pour lesquelles nous achetons autant de technologie en ce moment, et c'est l'un des principaux arguments publicitaires d'Apple : votre iPhone (ou iPad ou Mac) est tellement avancé que son utilisation est « magique ». Mais rien n'est vraiment magique : le matériel et le logiciel sont tellement avancés qu'ils font des tas de choses dont on ne veut pas se préoccuper, et on a ainsi l'impression que c'est magique. Apple fait donc des tas de choses avec nos données pour nous donner cette impression de magie, et parfois, ça ressemble plus à de la sorcellerie ! C'est sûrement ainsi qu'ont dû le percevoir les victimes du *celebgate* déjà abordé au deuxième chapitre, scandale de la fin août 2014 où des photos de célébrités nues ont fuité sur internet. Dans la plupart des cas, les victimes ont vu des photos très intimes prises avec leur propre smartphone publiées sur le web, alors que leur téléphone n'avait pas été volé. Cela a dû être une sacrée surprise de réaliser que les photos ne restent pas dans leur appareil mais sont envoyées de façon invisible à des serveurs d'Apple, d'où elles ont été prises pour être dévoilées à un public de voyeurs.

Apple a sciemment mis en place cette fonctionnalité, principalement pour deux raisons : sauvegarder les photos en cas de perte ou de vol du téléphone ; permettre la synchronisation et le partage des fichiers entre les différents appareils de la marque appartenant au même utilisateur.

Apple n'a pas grand-chose à se reprocher à ce sujet, hormis une sécurisation existante, mais trop faible, des copies de sauvegarde, qui semblent être la source des fuites de photos. Depuis, la sécurité a été augmentée par Apple. Mais il est bon que l'utilisateur sache que les avantages « magiques » qu'il peut retirer de l'usage de ses multiples appareils se fondent sur une captation de données qui n'apparaît jamais clairement.

Le problème de l'App Store

Une autre pratique d'Apple retire aux utilisateurs la possibilité de contrôler leur informatique : l'App Store d'Apple est l'unique façon d'installer une application sur un iPhone et un iPad. Du coup, tout développeur souhaitant diffuser une application doit voir cette application validée par Apple selon des critères parfois arbitraires. Voici trois exemples d'applications qui ont été acceptées puis refusées par Apple. Notons que toutes sont légales dans la plupart des pays :

> Baby Shaker. Une application (de très mauvais goût) qui permet de faire taire (de façon définitive) un bébé qui pleure en secouant le téléphone.
>
> Le quotidien allemand Bild, plus gros tirage d'Europe occidentale avait l'habitude de mettre une jeune femme a demi-dévêtue en couverture. Bild a dû faire des couvertures spécifiques pour que sa version électronique soit acceptée par l'App Store, parce que la nudité, même partielle n'est pas autorisée par Apple. C'est très préoccupant pour la liberté de la presse… D'autres journaux ont subi les mêmes déboires.

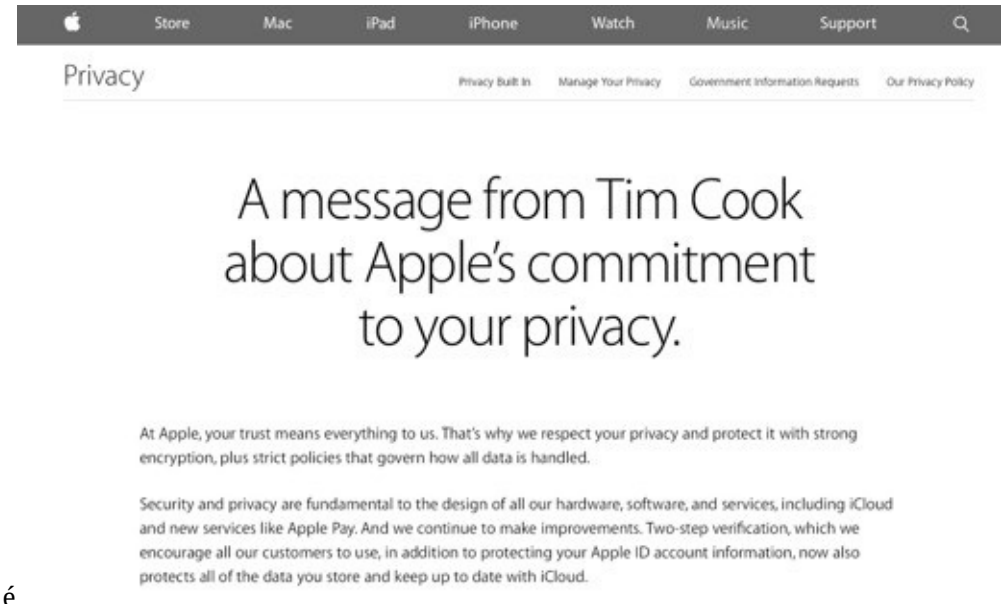
Mark Fiore, caricaturiste politique, a vu son application censurée par Apple sous prétexte qu'il « *se moquait de gens célèbres* ». Ce n'est que lorsqu'il a reçu le prix Pulitzer (plus haute distinction pour un journaliste) que l'affaire a été remarquée par la presse, ce qui a forcé Apple à faire marche arrière. Mark Fiore a alors déclaré 75 : « *Mon appli a été approuvée, mais si quelqu'un en fait une meilleure que la mienne sans avoir le Pulitzer ? Faut-il nécessairement avoir un buzz médiatique pour qu'une application à contenu politique soit admise par l'App Store ?* »

Le problème de cette approche, c'est qu'Apple choisit ce qu'on a la possibilité d'utiliser ou pas sur son iPhone et iPad. Là, on ne parle même plus de contrôle par l'utilisateur, mais carrément de censure !

Les promesses d'Apple

C'est un fait, Apple est une société particulièrement opaque à de nombreux points de vue, cultivant le secret. Cette opacité s'étend en particulier au code source de ses logiciels, du système d'exploitation du Mac et de l'iPhone à leurs applications et aux services comme iCloud.

Aussi, quand on constate un problème de sécurité ou qu'on soupçonne Apple de transmettre nos données à des tiers, par exemple la NSA, la seule défense d'Apple est d'affirmer que ça n'est pas vrai. Bien sûr, l'enjeu est de taille, donc la communication est faite par les plus hautes instances de la société, en particulier Tim Cook lui-même, le PDG successeur de Steve Jobs, en complément d'explications techniques 76.


Store
Mac
iPad
iPhone
Watch
Music
Support
Privacy
Privacy Built In
Manage Your Privacy
Government Information Requests
Our Privacy Policy
A message from Tim Cook about Apple's commitment to your privacy.
At Apple, your trust means everything to us. That's why we respect your privacy and protect it with strong encryption, plus strict policies that govern how all data is handled.
Security and privacy are fundamental to the design of all our hardware, software, and services, including iCloud and new services like Apple Pay. And we continue to make improvements. Two-step verification, which we encourage all our customers to use, in addition to protecting your Apple ID account information, now also protects all of the data you store and keep up to date with iCloud.
é

Copie d'écran : « Une lettre de Tim Cook sur l'engagement d'Apple pour protéger votre vie privée. »
Capture d'écran du site d'Apple : lettre de son PDG Tim Cook sur l'engagement d'Apple pour protéger votre vie privée.

Apple contre le FBI

Entre décembre 2015 et mars 2016, une série d'événements a mis Apple sous les feux de la rampe en

ce qui concerne la protection de la vie privée. En effet, le 2 décembre 2015, un couple tue 14 personnes à San Bernardino, Californie. La tuerie met l'Amérique en émoi et l'enquête est confiée au FBI. Le couple disposait de trois téléphones mobiles, dont deux sont détruits. Il reste un iPhone 5C dont le contenu pourrait révéler des indices sur d'éventuels commanditaires de l'attentat. Mais le contenu du téléphone est protégé par un code secret qui, au bout de 10 essais infructueux, pourrait effacer les données contenues dans l'iPhone. Le FBI demande donc à Apple de coopérer, ce que fait tout d'abord la marque à la pomme, en fournissant les sauvegardes du téléphone stockées dans son service iCloud. Il apparaît que, suite à une mauvaise manœuvre du FBI, ces données sont inexploitables. Le FBI demande alors à Apple de produire une version spécifique d'iOS, le logiciel qui fait fonctionner l'iPhone. En mettant à jour l'iPhone avec ce logiciel spécialement écrit et auquel on a retiré les fonctionnalités de protection des données, le FBI pourrait accéder au contenu du téléphone. Dans une longue « lettre à nos clients » 77, Apple refuse et explique sa position : fabriquer pour l'occasion une porte dérobée qui risquerait de tomber « dans les mauvaises mains » (criminelles ou appartenant à des États non démocratiques).

Entre le FBI et Apple, le bras de fer médiatique dure de longues semaines et touche de nombreux pays, y compris la France, où le député PS Yann Galut veut contraindre les groupes high-tech à coopérer avec la justice sur la question du chiffrement 78 et le député LR Éric Ciotti qui veut tout simplement interdire l'iPhone 79.

Malgré la pression médiatique et les menaces du FBI, Apple tient bon et démontre à cette occasion sa détermination à protéger les données des utilisateurs, d'autant plus que cette entreprise a mis en place des systèmes de chiffrement de ses smartphones qui font que dans bien des cas, elle n'a, elle-même, pas accès aux données des utilisateurs 80.

En conclusion, on peut reprocher de nombreuses choses à Apple, à commencer par son opacité, sa relation compliquée avec le logiciel libre, sa volonté de censurer l'App Store. Pourtant, son modèle d'affaire qui n'est pas lié à la publicité ciblée et sa volonté de ne pas fouiller dans les données de ses utilisateurs lui ont permis de mettre en place une approche de la vie privée qui distingue cette entreprise de ses concurrents, lui permettant ainsi de tenir tête au FBI.

18. Smartphones et Cloud

Avec l'arrivée du smartphone, il est devenu nécessaire de synchroniser des fichiers entre notre ordinateur et notre smartphone, comme par exemple notre agenda, nos notes, nos documents… Pour cela, il faut que les deux soient allumés et connectés à internet au même moment. Comme ça n'est pas toujours le cas pour les ordinateurs portables, on utilise un ordinateur qui est en permanence allumé et connecté à internet, un serveur. Pour des raisons commerciales, on appelle cela le « cloud », ou en français « l'informatique dans les nuages ». C'est une façon rassurante de présenter les choses, mais concrètement, le *cloud*, c'est l'ordinateur de quelqu'un d'autre, ni plus, ni moins. Cela veut dire qu'on ne le contrôle pas du tout, et c'est bien souvent par son intermédiaire que nos données personnelles sont récoltées.

Les logiciels de nos ordinateurs aussi

Pour récupérer nos données sur les serveurs, plusieurs techniques sont utilisées par certaines grandes sociétés internet. Facebook, par exemple, offre un service gratuit. Google aussi, mais en allant plus loin : Google « offre » en plus des logiciels gratuits, comme le navigateur Chrome, qui, associé à un compte Gmail, collecte toutes sortes d'informations, comme les mots de passe des sites web, l'historique des pages web visitées, le texte saisi dans les formulaires, et ainsi de suite. Le document décrivant tout ce que fait Chrome et les données qu'il collecte fait 10 pages 81.

Les smartphones aussi

Google procède d'une manière très semblable avec les smartphones. En effet, Google développe le système d'exploitation pour smartphones appelé Android et l'offre gratuitement aux fabricants de téléphones comme Samsung, LG, HTC et à peu près tous les autres sauf Apple. Si vous avez un smartphone, comme sept Européens de l'Ouest sur dix, il y a de grandes chances pour qu'il soit équipé du logiciel Android de Google, qui représente 74,7 % des ventes. Apple est deuxième à 21,5 %. Le troisième, Windows Phone de Microsoft, est en baisse à 3,6 %. Les autres se partagent les 0,2 % restants.

Si Google offre gratuitement Android à des géants comme Samsung ou LG, ça n'est pas par bonté d'âme, c'est parce que ces fabricants sont contractuellement obligés de livrer leur matériel avec des applications pré-installées, comme Google Maps (qui sait où on se trouve), Google Search (pour savoir ce qu'on cherche et donc de quoi on se préoccupe), et de Google Chrome (voir ci-dessus). Le fait de ne pas avoir à payer Android permet aux fabricants d'obtenir des prix compétitifs vis-à-vis d'Apple. Mais du coup, Google récolte des quantités phénoménales de données sur chaque utilisateur, sans que celui-ci s'en doute, jusqu'à ce qu'il s'en rende compte comme je le décrivais dans l'introduction de cet ouvrage, avec par exemple Google Location History (traçage des déplacements de l'utilisateur) ou Google Now, qui anticipe vos besoins en information.

En ce sens, les logiciels de Google, d'Android à Chrome, sont de véritables chevaux de Troie : ils ressemblent à des cadeaux extraordinaires mais n'existent que pour servir celui qui les a fabriqués,

Google.

Les applications des smartphones aussi

Le piège de la gratuité fonctionne aussi très bien avec les applications pour smartphones. Je n'ai pas eu à chercher longtemps pour trouver une application des plus anodines pour Android, « Brightest Flashlight Free », qui est franchement louche. L'application est pourtant toute simple, puisque qu'elle allume l'écran et le flash de la caméra pour servir de lampe de poche. Et elle affiche des publicités. Pourtant, quand on regarde d'un peu plus près, on en arrive à s'interroger sur les permissions dont elle a besoin :

position du téléphone par GPS et wifi ;

accès aux photos et documents stockés dans le téléphone, y compris pour les supprimer ;

identité du téléphone ;

accès à internet.

Autrement dit, l'application veut savoir où on se trouve, qui nous sommes, peut lire tous nos documents et les envoyer où elle veut sur internet. Tout ça pour allumer le flash de la caméra ?

Sachant que ces précisions sont affichées avant d'installer l'application, on se dit que toute personne raisonnable refuserait d'installer un espion pareil. Pourtant, l'application a été installée plus de 50 millions de fois.

Quand on sait qu'un smartphone dispose d'une caméra, d'un micro, d'un GPS et de capteurs de mouvement, on imagine la quantité de données qu'il peut amasser pour les transmettre à des serveurs « dans le Cloud » sur internet.

19. Internet des objets, quantified self et beacons

Au-delà des PC et des smartphones, qui sont déjà très répandus, une nouvelle vague d'appareils connectés à internet est sur le point de déferler sur le monde, celle de l'internet des objets.

Les objets du quotidien : voiture, télévision, réfrigérateur

Une nouvelle génération d'objets du quotidien est en train d'apparaître. On les affuble du préfixe « smart » pour les rendre plus attirants, mais la valeur ajoutée de leurs nouveaux services comporte de grands risques en termes de fuites de données, sans compter le fait que les logiciels qui les font fonctionner sont souvent propriétaires : on ne peut presque jamais les voir, les comprendre, les modifier pour les adapter à nos besoins.

La voiture

C'est déjà presque un classique dans certains pays comme les États-Unis, où les assureurs comme la société Progressive proposent de mettre un GPS connecté à internet, promettant une économie jusqu'à 30 % dans certains cas. Un client, Joe Manna, a essayé pendant six mois, pour finalement économiser 1 dollar en tout 82. Les données (horaires, freinages) sont transmises à l'assurance en temps réel par le réseau mobile. Joe Manna conclut son expérience par ces mots : « *Débrancher le GPS de Progressive est comparable à la sensation que doit éprouver un chien quand on lui retire son collier*. »

Mais une nouvelle génération comme la Tesla Model S, magnifique voiture électrique de luxe disposant d'une immense tablette tactile en guise de tableau de bord, et doté de moteurs fournissant entre 376 et 691 chevaux, va beaucoup plus loin. La publicité fait étalage de la technologie embarquée, mais passe soigneusement sous silence quelles données sont collectées par cette voiture connectée à internet et envoyées au constructeur. Il aura fallu attendre un incident avec un journaliste 83 pour découvrir que Tesla accumule les données avec voracité : vitesse instantanée, niveau de charge de la batterie, évolution de l'autonomie restante, température intérieure du véhicule, et probablement beaucoup d'autres paramètres qui ne sont pas indiqués, sachant que la voiture est fièrement équipée de Google Maps, application qui permet à Google de pister chaque utilisateur. Ceci est confirmé par la *privacy policy* de Tesla 84 dont la lecture donne un peu le tournis tellement la collecte de données est importante.

Pour conclure sur ce sujet, voici la conclusion d'un journaliste de la revue *Forbes* 85 à propos de Tesla :

Nous devons réfléchir dès maintenant pour savoir qui peut accéder à ces données et comment est géré cet accès. En effet, dans un jour prochain, nos voitures seront un problème pour notre vie privée comme nos smartphones le sont déjà.

La télévision intelligente

Les grands constructeurs d'appareils ménagers se sont jetés sur le marché de la télévision numérique,

cherchant à pousser les consommateurs à renouveler leur poste. Grâce à Samsung, le cauchemar a déjà commencé : début 2015, la presse a compris que les Smart-TV, équipées d'une commande vocale, impliquaient l'acceptation d'une *privacy policy* 86 qui rappelait nettement le roman *1984* de George Orwell :

Samsung peut écouter des commandes vocales et des textes associés via votre télévision de façon à vous fournir des fonctionnalités de reconnaissance vocale, mais aussi pour évaluer et améliorer des fonctionnalités. Nous vous prions de prendre conscience que si les mots prononcés contiennent des informations sensibles ou personnelles, ces informations seront aussi capturées et transmises à une tierce partie via la reconnaissance vocale.

Il est apparu après quelques recherches que non seulement ces données sont transmises à un sous-traitant, mais qu'en plus elles transitent sur internet sans être chiffrées, contrairement à ce qu'indiquait Samsung 87.

Avec la Smart-TV, on va finir par regretter que ça ne soit pas les programmes télé qui deviennent intelligents et les télévisions qui restent stupides !

La console de jeux

Avec la console de jeux XBox, Microsoft a frappé un grand coup en proposant un accessoire, Kinect, qui permet de se passer d'une manette pour jouer. Mais Kinect, ce sont surtout deux caméras qui filment ce qui se passe dans la pièce. On imagine les dérapages possibles, surtout quand on voit que Microsoft a déposé un brevet 88 qui permet de compter les gens présents devant la télé afin d'empêcher la lecture du DVD s'ils sont trop nombreux.

Le « quantified self »

Depuis quelques années, une nouvelle catégorie de produits est en train de devenir populaire : les capteurs électroniques mesurant notre santé. Portés en permanence sur soi, ils mesurent le nombre de pas, les calories dépensées, les heures de sommeil, éventuellement le pouls et bien d'autres choses. Certaines marques proposent aussi des balances connectées qui mesurent notre poids et le pourcentage de graisse dans le corps. Toutes ces données sont envoyées aux serveurs des fabricants. À qui appartiennent ces données ? Comment sont-elles utilisées, les clients y ont-ils accès ? La réponse semble changer au cours du temps. Prenons le cas de la société Fitbit, leader du marché.

En 2011, il est apparu que trop de données personnelles sur les utilisateurs étaient disponibles via une simple recherche Google, y compris l'activité sexuelle des clients 89. Très rapidement, Fitbit a modifié son logiciel pour éviter de publier de telles données personnelles.

Dorénavant, ces données ne sont accessibles que par les utilisateurs, protégées par un mot de passe. Mais on ne peut y voir que les données jour par jour : impossible d'avoir accès à l'ensemble des données brutes pour faire des analyses personnelles, par exemple pour savoir le moment de la journée où l'on fait le plus d'exercice, etc. En fait, c'est possible, mais il faut pour ça payer un abonnement supplémentaire de 44,99 € par an, soit à peu près le prix du capteur (le modèle Fitbit Zip vaut environ 60 €). Avoir à payer un supplément pour avoir accès à mes données ? Voilà qui ne manque pas d'air !

La lecture de la *privacy policy* 90 de Fitbit indique que nos données ne peuvent être vendues qu'après qu'elles aient été anonymisées (pour que l'acheteur ne sache pas à qui elles correspondent). De même, nos données personnelles peuvent également être vendues si la société est elle-même revendue ou réorganisée. Autrement dit, quand ils veulent (les réorganisations peuvent être décidées facilement par la direction).

Si on déchiffre le message, c'est « ne vous en faites pas, vos données sont en sécurité chez nous, sauf si on décide du contraire. Mais vous pouvez en avoir une copie en payant tous les ans ».

Les nouveaux objets dans la maison

La société française Sense propose un produit très novateur appelé Mother, qui fonctionne avec des capteurs connectés. Dans la vidéo de présentation, on voit les capteurs compter le nombre de cafés bus, le temps de sommeil de chacun, l'heure de retour à la maison du gamin, le temps qu'il passe à se brosser les dents, les ouvertures et fermetures de la porte, et des dizaines de données du même genre. Les objets du quotidien dotés de capteurs recueillent des données sur toutes les personnes vivant à la maison. Mais où vont ces données ?

J'ai cherché la *privacy policy* 91 de la société Sense et j'ai eu beaucoup de plaisir à la lire. Parce qu'elle était courte et compréhensible : 19 mots seulement ! Du coup, je la recopie en entier :

Toutes les données captées par des appareils que vous achetez sont à vous. Rien qu'à vous. Point final.

C'est de toute évidence une exception dans le monde dans lequel nous vivons aujourd'hui, et aussi un soulagement : cela montre que c'est possible !

Malheureusement, c'est une exception, mais il nous appartient de nous assurer que celle-ci va devenir la règle, par exemple en choisissant les produits et services qui sont respectueux de nos données.

Dans les magasins, dans la rue et les centres commerciaux : les beacons

Pour finir, voici que se développe un nouveau type de capteurs sur lesquels nous n'avons aucun contrôle : ceux qui sont dans notre environnement. On appelle ceux-ci les *beacons* (en français : « balises »). Ce sont des capteurs souvent destinés au marketing. Ils peuvent être placés dans les magasins, les centres commerciaux, ou dans la rue. Ils sont capables d'envoyer des messages sur les smartphones équipés de l'application spécifique, mais ils sont aussi utilisés pour suivre les mouvements des consommateurs. Il y a eu en octobre 2014 un scandale à New York 92, où l'on a découvert un réseau de *beacons* installés dans les cabines téléphoniques de la ville par une société de marketing. Suite à des révélations dans la presse, ceux-ci ont été retirés.

On commence à trouver des *beacons* en France : le centre commercial La Vallée Village, situé près de DisneyLand Paris a des affiches à l'entrée prévenant les visiteurs que leurs mouvements sont susceptibles d'être tracés lors de leurs visites. J'ai voulu prendre une photo du panneau, mais un vigile m'en a empêché.

Le Figaro semble enthousiaste 93 :

Aide à la navigation et à l'information, les beacons sont aussi des vecteurs de promotion, bien plus

attractifs qu'un panneau publicitaire. Yeux rivés sur leurs écrans, les consommateurs sont de plus en plus imperméables aux colonnes Morris et autres enseignes murales. Avec les beacons, en une fraction de seconde, une marque peut venir agiter sa dernière réduction sous le nez de ses clients potentiels.

La CNIL, pour sa part, est plus circonspecte quant aux données collectées par les *beacons* 94 : « *Les données doivent être anonymisées immédiatement* ».

En effet, combinés à des caméras, les *beacons* peuvent servir à mesurer l'audience des panneaux publicitaires, comme on en trouve dans le métro parisien. À leur sujet, voici comment la CNIL décrit leur fonctionnement :

Ces dispositifs reposent sur des caméras placées sur des panneaux publicitaires. Ils permettent de compter le nombre de personnes qui regardent la publicité et le temps passé devant celle-ci, d'estimer leur âge et leur sexe, voire d'analyser certains comportements (en suivant par exemple les déplacements du regard de la personne sur les différentes parties de la publicité).

Comment se protéger de ceci ? En faisant confiance aux publicitaires quant à leur respect des exigences de la CNIL ? Ou alors en éteignant nos téléphones portables ?

20. Les services de renseignement

Les services de renseignement existent depuis longtemps, et l'on peut comprendre l'importance de leur mission qui participe à la sécurité nationale. Le code de la Défense précise qu'ils doivent « *identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République* ».

Cette mission est respectable et nécessaire dans le cadre démocratique, dans la mesure où elle est légale et ciblée. La surveillance de masse, comme expliqué au chapitre 8 (« la vie privée dans la loi ») du présent ouvrage, est illégale et contraire à l'éthique.

Pourtant, la tentation de la surveillance de masse est grande, comme le fantasme de surveiller tout le monde, tout le temps, pour arriver au risque zéro et prévenir les problèmes avant qu'ils n'arrivent.

Mais le risque zéro, c'est surtout zéro liberté. C'est un état policier.

La surveillance de masse est-elle efficace ?

Il semblerait que surveiller toute la population ne soit pas la solution au problème du terrorisme, prétexte évoqué pour justifier la surveillance de masse. Ainsi, en décembre 2013, un membre de la Maison Blanche avouait que les milliards de dollars investis par la NSA dans l'écoute des Américains n'avaient jamais empêché le moindre acte terroriste 95.

Plus récemment, en France, lors des attentats islamistes de janvier 2015, il est apparu que deux des trois djihadistes concernés avaient été surveillés par la police pendant plusieurs années 96. D'aucuns, pour excuser l'inefficacité des services pour empêcher ces attentats, expliquent qu'il y a trop de monde à surveiller, que c'est comme chercher une aiguille dans une botte de foin. Mais avec la surveillance généralisée, espère-t-on que multiplier la quantité de foin va faciliter la recherche de l'aiguille ?

La centralisation des données rend économiquement possible la surveillance de masse

Pour un État, il est impossible car trop coûteux d'organiser lui-même la surveillance de chaque individu : il faudrait mettre des micros, des caméras, des capteurs partout, puis centraliser les données pour enfin les analyser.

Pourtant, cette tâche titanesque est rendue possible grâce à la coopération active de presque tout le monde : en nous équipant nous-mêmes de capteurs (smartphones et autres), en mettant les données générées dans quelques grands silos qui sont économiquement rentables (Google, Facebook, FitBit, opérateurs télécoms et autres), nous rendons économiquement possible la surveillance de masse en abaissant son coût. Au lieu d'organiser la collecte de données, ce qui serait trop coûteux, les services de renseignement peuvent se contenter de parasiter un système auquel nous participons et que nous finançons sans mesurer les conséquences.

La situation en France avant 2015

Jusqu'en 2015, la surveillance de masse est interdite en France. En effet, jusqu'à la Loi renseignement, le droit écrit limite les techniques de renseignement sur le territoire français à l'écoute ciblée des lignes de téléphone fixes. En effet, la loi encadrant les écoutes date d'avant internet et les téléphones mobiles. Si les services de renseignement voulaient placer quelqu'un sous écoute, c'était donc forcément sur une ligne fixe, et chaque demande était validée par un juge et contrôlée par une autorité administrative indépendante, la CNCIS 97. Ce système a été mis en place suite au scandale dit des « écoutes de l'Élysée » 98.

Techniquement, il existe des dispositifs appelés *IMSI-Catchers* qui permettent de capter les communications passées depuis des terminaux mobiles GSM. Le concept est très simple : il s'agit d'une fausse antenne GSM qui capte les signaux des mobiles, récupère certaines informations (identifiants des téléphones dans le secteur, appels et SMS passés et reçus, voire les communications informatiques pour certains modèles). On apprend dans un article du *Canard Enchaîné* 99 qu'une douzaine d'équipements de ce type étaient utilisés. Comme le précise *Le Canard*, « *L'IMSI-Catcher n'a jamais été autorisé pour les écoutes administratives car ce système est jugé bien plus attentatoire aux libertés qu'une interception téléphonique classique* ». La CNCIS « *s'est émue* mezza voce *de ces violations de la loi* ».

Depuis 2015

La situation a beaucoup changé en 2015. Les ministères de l'Intérieur et de la Défense travaillaient depuis plusieurs mois déjà à une loi dite « Renseignement » qui visait à moderniser les règles encadrant la collecte de renseignements. Les attentats de janvier 2015 (Charlie Hebdo et la supérette Hyper-Casher) ont donné un prétexte pour aller encore plus loin et instaurer la surveillance de masse de l'internet français. En effet, parmi les points saillants de la Loi Renseignement, on note :

- la possibilité d'utiliser des « boîtes noires » (le terme du gouvernement !), installées sur les serveurs, qui pourront surveiller des pans entiers de l'internet français pour « détecter les comportements suspects » des internautes ;
- l'autorisation d'utiliser les *IMSI-catchers* ;
- le remplacement de la CNCIS par une autre autorité, la CNCTR (Commission nationale de contrôle des techniques de renseignement), qui contrairement à la précédente, n'a pas de quota d'écoutes.

La levée de boucliers contre cette loi fut sans précédent. On a vu ainsi un large front d'opposition se constituer, composé d'acteurs aussi divers que l'ONU, la CNIL, le Conseil National du Numérique, les acteurs du numérique, et des associations comme la Ligue des Droits de l'Homme, Amnesty International, Reporters sans Frontières, le Syndicat National des Journalistes et même la Fédération des Motards en Colère ! Rien n'y fera, les débats autour de cette loi, grâce à l'émotion provoquée par les attentats de janvier 2015, ne pourront pas arrêter l'adoption du texte en juillet 2015, le gouvernement ayant eu recours à une procédure d'urgence.

Alors, que faire face à la surveillance de masse ?

Pour empêcher la surveillance de masse, deux approches complémentaires peuvent et doivent être utilisées.

Approche politique : renforcer les institutions

Tout d'abord, il convient de mettre en place des mécanismes institutionnels capables d'éviter la mise en place d'un État policier. Ici, la démarche est celle d'un citoyen informé et acteur de la vie politique : il faut se tenir informé (si vous lisez cet ouvrage, c'est que vous avez probablement déjà cette démarche !), ne pas succomber aux discours sécuritaires qui, jouant sur l'émotion, mènent à des lois liberticides. Il faut s'assurer que les institutions fonctionnent bien.

Je ne vais pas m'étendre sur ce sujet, qui dépasse le thème de ce livre, mais je suggère juste aux lectrices et lecteurs de se rapprocher d'une association appelée La Quadrature du Net, qui fait un travail remarquable d'information et d'action sur le sujet. Au passage, j'encourage mes lecteurs à faire un don à la Quadrature du Net pour qu'elle puisse continuer son action dans le temps avec encore plus de force.

Approche technique : construire des systèmes résilients qui nous protègent

Au-delà de la loi et de la politique, il est possible d'imaginer des systèmes informatiques qui rendraient très difficiles la surveillance de masse. C'est ce que je vous propose d'aborder dans la troisième partie de ce livre.

Notes

49 Extrait du document « Le projet GNU » – https://www.gnu.org/gnu/thegnuproject.html.

50 Le projet GNU recense sur une page web « les portes dérobées du logiciel privateur » – https://www.gnu.org/philosophy/proprietary-back-doors.html.

51 Windows NT 4 Service Pack 5, qui avait été publié sans être débarrassé des données de débogage symbolique, contenait donc les noms des variables utilisées, dont une intitulée _NSAKEY (clé NSA), qui contenait une clé publique de 1024 bits. On ignore vraiment à quoi servait une telle clé – https://en.wikipedia.org/wiki/NSAKEY.

52 La messagerie Lotus Notes permettait le chiffrement avec une clé de 64 bits dont 26 étaient joints de manière chiffrée à chaque message. La NSA disposait de la clé permettant de déchiffrer cette partie de la clé, ce qui lui facilitait grandement la tâche si elle voulait décrypter les messages, là où d'autres organisations et gouvernements devaient décrypter du 64 bits – https://en.wikipedia.org/wiki/IBM_Notes#Security.

53 « Le logiciel Skype interdit de séjour dans l'enseignement supérieur et la recherche » suite à une recommandation par le secrétariat général à la défense nationale, *ZDNet*, 27 septembre 2005 – http://www.zdnet.fr/actualites/skype-interdit-de-sejour-dans-l-enseignement-superieur-et-la-recherche-39267873.htm.

54 Avec ironie, l'Environmental Protection Agency des États-Unis avait, peu de temps avant que l'affaire n'éclate au grand jour, suivi les pressions du lobby automobile pour empêcher que le code source des logiciels embarqués ne soit ouvert, au prétexte que cela pourrait inciter des amateurs à bricoler leur logiciel pour outrepasser les normes de pollution. Un bel exemple d'aveuglement.« VW scandal highlights irony of EPA opposition to vehicle software tinkering » (Le scandale Volkswagen met ironiquement en lumière l'opposition de l'EPA au contrôle des logiciels automobiles embarqués), *Ars Technica*, 21 septembre 2015 – http://arstechnica.com/tech-policy/2015/09/vw-scandal-highlights-irony-of-epa-opposition-to-vehicle-software-tinkering/.

55 « L'iPad 2, aussi puissant qu'un supercalculateur (de 1985) », *MacGénération*, 10 mai 2011 – http://www.macg.co/2011/05/lipad-2-aussi-puissant-quun-supercalculateur-de-1985-57626.

56 « Toute la puissance informatique de la mission Apollo dans une seule requête Google ! », *L'Usine Nouvelle*, 29 août 2012 – http://www.usinenouvelle.com/article/toute-la-puissance-informatique-de-la-mission-apollo-dans-une-seule-requete-google.N180825.

57 https://www.facebook.com/policy.php.

58 https://www.facebook.com/about/privacy/your-info.

59 http://www.google.fr/intl/fr/policies/privacy/.

60 Ces mots ont été recueillis par les auteurs du livre *Les dirigeants face au changement*, Éd. du Huitième jour, 2004. Cette citation a soulevé une large polémique, mais chacun s'entend à reconnaître qu'elle décrit précisément le métier des chaînes de télévision. Un reportage de Canal + interroge des annonceurs sur cette citation en forme de dévoilement – https://youtu.be/UYrFAQsEdp0.

61 Chiffres 2015. Voir ligne Total Operating Expense – http://finance.yahoo.com/quote/FB/financials.

62 Chiffres 2015 donnés par JournalduNet : http://www.journaldunet.com/ebusiness/le-net/1125265-nombre-d-utilisateurs-de-facebook-dans-le-monde/.

63 http://geekandpoke.typepad.com/geekandpoke/2010/12/the-free-model.html.

64 Ce fut l'expérience de Jason Kincaid qui découvre que certaines données très personnelles sont partagées avec le support technique d'Evernote – http://jasonkincaid.net/2014/01/evernote-the-bug-ridden-elephant/.

65 Des pirates affirment avoir eu accès aux données de près de 7 millions de comptes Dropbox. « 7 millions de mots de passe détournés, Dropbox dément » *ZDNet*, 14 octobre 2014 – http://www.zdnet.fr/actualites/7-millions-de-mots-de-passe-detournes-dropbox-dement-39807779.htm.

66 « Viré de Facebook, la justice s'en mêle ! », *01Net*, 18 avril 2012 – http://www.01net.com/actualites/vire-de-facebook-la-justice-s-en-mele-564564.html.

67 « Yann Moix, viré de Facebook, crie à la censure », *Slate.fr*, 9 février 2010 – http://www.slate.fr/story/17097/yann-moix-vire-de-facebook-crie-la-censure.

68 https://evernote.com/intl/fr/legal/tos.php.

69 « Spy Agencies Probe Angry Birds and Other Apps for Personal Data » (Les agences d'espionnage fouillent les données personnelles dans Angry Birds et d'autres apps), *ProPublica*,27 janvier 2014 – https://www.propublica.org/article/spy-agencies-probe-angry-birds-and-other-apps-for-personal-data.

70 « Tarification iCloud » – https://www.apple.com/fr/icloud/.

71 « E.T. Phone Home ? » (E.T. téléphone maison ?) – https://github.com/fix-macosx/yosemite-phone-home.

72 « Edward Snowden refuse d'utiliser un iPhone à cause du mouchard », *Numerama*, 24 janvier 2015 – http://www.numerama.com/magazine/31997-mouchard-iphone.html.

73 Voir la fiche du programme DROPOUTJEEP de la NSA sur le site nsa-observer.net – https://www.nsa-observer.net/category/attack%20vector/family/software/name/DROPOUTJEEP.

74 D'après Wikipédia, « dans la mythologie grecque, l'épisode du cheval de Troie est un événement décisif de la guerre de Troie. À l'initiative d'Ulysse, des guerriers grecs réussissent à pénétrer dans Troie, assiégée en vain depuis dix ans, en se cachant dans un grand cheval de bois, harnaché d'or, offert aux Troyens. Cette ruse de guerre entraîne la chute de la ville et permet le dénouement de la guerre » – https://fr.wikipedia.org/wiki/Cheval_de_Troie.

75 « Apple App Store Bans Pulitzer-Winning Satirist for Satire » (L'App Store d'Apple censure le caricaturiste ayant gagné le Pulitzer), *Wired*, 15 avril 2010 – http://www.wired.com/2010/04/apple-bans-satire/.

76 Livre blanc de septembre 2015, intitule « iOS Security » et téléchargeable depuis http://www.apple.com/business/docs/iOS_Security_Guide.pdf.

77 « A Message to Our Customers » (Lettre à nos clients) – http://www.apple.com/customer-letter/.

78 « L'affaire San Bernardino déteint en France », Clément Boic, *Itespresso*, 29 février 2016 – http://www.itespresso.fr/smartphones-chiffres-affaire-san-bernardino-deteint-france-122722.html.

79 « Lutte contre le chiffrement : Ciotti surenchérit et veut interdire l'iPhone », Guillaume Champeau, *Numerama*, 29 février 2016 – http://www.numerama.com/politique/149077-lutte-contre-le-chiffrement-ciotti-surencherit-et-veut-interdire-liphone.html.

80 « Comment fonctionne le chiffrement des données sur iPhone », Alexis Piraina, *Numerama*, 19 février 2016 – http://www.numerama.com/tech/146674-comment-fonctionne-le-chiffrement-des-donnees-sur-iphone.html.

81 Avis de Confidentialité Google Chrome – https://www.google.fr/chrome/browser/privacy/.

82 « What Every Driver Needs to Know about Progressive Snapshot » (Ce que chaque conducteur devrait savoir sur Progressive Snapshot), 21 juin 2014 – https://blog.joemanna.com/progressive-snapshot-review/.

83 « A Most Peculiar Test Drive » (Un essai très particulier), Elon Musk, *Tesla blog*, 13 février 2013 – https://www.teslamotors.com/blog/most-peculiar-test-drive.

84 « Customer Privacy Policy » (Politique concernant la vie privée des clients), *Tesla* – https://www.teslamotors.com/about/legal.

85 « The Big Privacy Takeaway From Tesla vs. The New York Times » (Ce qu'on peut retenir sur la vie privée dans ce qui oppose Tesla au New York Times), Forbes, 19 février 2013 – http://www.forbes.com/sites/kashmirhill/2013/02/19/the-big-privacy-takeaway-from-tesla-vs-the-new-york-times/.

86 « Samsung Global Privacy Policy – SmartTV Supplement » (Politique globale de Samsung sur la vie privée – supplément SmartTV) – http://www.samsung.com/uk/info/privacy-SmartTV.html.

87 « Samsung lied – its smart TV is indeed spying on you and it is doing nothing to stop that » (Samsung a menti : sa Smart TV nous espionne bien et ils ne font rien pour changer cela), *BetaNews*, 19 février 2015 – http://betanews.com/2015/02/19/samsung-lied-its-smart-tv-is-indeed-spying-on-you-and-it-is-doing-nothing-to-stop-that/.

88 « Copyright Industry Madness Takes Six Years To Catch Up With The Worst Satire Of It » (La folie de l'industrie du copyright devient réalité 6 ans après qu'on ait imaginé sa pire caricature), *Falkvinge.net*, 10 novembre 2012 – http://falkvinge.net/2012/11/10/copyright-industry-reality-takes-six-years-to-catch-up-with-the-worst-satire-of-it/.

89 « Fitbit users are unwittingly sharing details of their sex lives with the world » (Les utilisateurs de FitBit partagent publiquement et sans le savoir des détails de leur vie sexuelle), *TheNextWeb*, 3 juillet 2011 – http://thenextweb.com/insider/2011/07/03/fitbit-users-are-inadvertently-sharing-details-of-their-sex-lives-with-the-world/.

90 Fitbit Privacy Policy – https://www.fitbit.com/uk/privacy.

91 « Mother, une maman, mais en mieux » Dossier de Presse Sen.se, décembre 2013 (notamment p. 9) – https://www.sen.se/static/press/Sense_Mother_&_the_Motion_Cookies_Dec_2013.pdf.

92 « New York City Kills Hidden Phone Booth Devices » (La ville de New York tue les capteurs cachés dans les cabines téléphoniques), *BuzzFeed*, 6 octobre 2014 – http://www.buzzfeed.com/josephbernstein/new-york-city-to-advertising-contractor-take-down-secretly-i.

93 « Les beacon, traqueurs invisibles de clients », *Le Figaro*, 12 décembre 2014 – http://www.lefigaro.fr/secteur/high-tech/2014/12/12/32001-20141212ARTFIG00099-les-beacon-traqueurs-invisibles-de-clients.php.

94 « Mesure de fréquentation et analyse du comportement des consommateurs dans les magasins », CNIL, 19 août 2014 – https://www.cnil.fr/fr/mesure-de-frequentation-et-analyse-du-comportement-des-consommateurs-dans-les-magasins.

95 « NSA Program Stopped No Terror Attacks, Says White House Panel Member » (Le programme de la NSA n'a empêché aucune attaque terrorriste, affirme un conseiller de la Maison blanche), Interview de Geoffrey Stone, professeur de droit à l'université de Chicago, par *NBC News*. Rapporté par *Information Clearing House*, 20 décembre 2013 – http://www.informationclearinghouse.info/article37174.htm.

96 « La surveillance des frères Kouachi s'était arrêtée il y a six mois », *L'Obs*, 11 janvier 2015 – http://tempsreel.nouvelobs.com/charlie-hebdo/20150110.OBS9696/charlie-hebdo-la-surveillance-des-freres-kouachi-s-etait-arretee-il-y-a-six-mois.html.

97 Commission Nationale de Contrôle des Interceptions de Sécurité – https://fr.

wikipedia.org/wiki/Commission_nationale_de_contr%C3%B4le_des_interceptions_de_s%C3%A9curit%C3%A9.

98 Le Président de la République, François Mitterrand, avait mis en place des écoutes téléphoniques illégales de 1983 à 1986 via une cellule dite « antiterroriste » de l'Élysée, qui en réalité visait principalement à éviter des révélations sur Mazarine Pingeot, fille naturelle du président.

99 « La loi sur les écoutes court-circuitée par un drôle de gadget », *Le Canard Enchaîné*, 4 février 2015, p. 3.

Partie III

Un autre réseau est possible

Inventer une approche de l'informatique en réseau limitant la surveillance

Partie III
Un autre réseau est possible

Inventer une approche de l’informatique en réseau limitant la surveillance

21. Sept principes pour reprendre le contrôle

Pour reprendre la main sur l'informatique, il faut inventer des systèmes informatiques contrôlables par l'utilisateur et seulement par lui. Appelons ces systèmes des SIRCUS (Systèmes Informatiques Redonnant le Contrôle aux Utilisateurs).

Pour qu'un SIRCUS puisse exister, il faut reprendre la main autant que possible sur chacun des composants : le matériel, le logiciel et les réseaux.

J'établis là quelques grands principes qu'il faut explorer pour parvenir à une solution idéale. Notons qu'il n'est pas nécessaire d'avoir une solution parfaite pour commencer à avancer dans cette direction.

Principes de base : le fondement technologique

1. Du logiciel libre

Commençons par l'essentiel : le logiciel. Pour que l'utilisateur sache ce qu'il fait (transparence), pour pouvoir le modifier si nécessaire, pour que nous en ayons le contrôle, le logiciel doit impérativement être un logiciel libre.

2. Le contrôle du serveur

Ensuite, il faut contrôler le matériel sur lequel tourne le logiciel. Pour le PC et le téléphone, cela semble aller de soi. Mais si on veut disposer des fonctionnalités de type *cloud*, avec des données accessibles en permanence depuis plusieurs appareils, il faut avoir accès à un serveur, une machine constamment connectée à internet. La solution idéale consiste à héberger soi-même son serveur. C'est ce qu'on appelle l'auto-hébergement.

3. Du chiffrement, encore du chiffrement !

Enfin, puisque des données vont transiter entre notre serveur et nos appareils (PC, smartphone, tablette), il faut qu'elles soient protégées des oreilles indiscrètes. Pour cela, l'utilisation du chiffrement (parfois appelée « cryptographie ») permet de rendre les données incompréhensibles pour les personnes non autorisées, soit quand elles sont stockées, soit quand elles transitent sur le réseau.

4. Éliminer le problème de fond : le profilage nécessaire à la publicité ciblée

La publicité ciblée est à l'origine du profilage de tous les internautes. Comme le dit Bruce Schneier 100, chercheur en sécurité : « *La surveillance est le modèle commercial de l'internet. Nous construisons des systèmes qui espionnent les gens en échange de services. C'est ce que les entreprises appellent du marketing.* » Il faut trouver un modèle économique pour l'internet qui ne repose pas sur le profilage des utilisateurs afin de leur rendre le contrôle.

Aller plus loin que les solutions existantes

Pour être adoptés, les futurs outils respectueux de la vie privée devront satisfaire à trois conditions (respectivement les cinquième, sixième et septième principes des SIRCUS) :

5. Proposer une ergonomie d'excellent niveau.

6. Être compatible avec les systèmes existants et à venir.

7. Apporter un « plus » concret et visible immédiatement qui les différenciera des offres actuelles.

Je vous propose d'explorer, dans les chapitres qui suivent, ces grands principes que nous tous, que nous soyons citoyens, développeurs, *startups* ou décideurs politiques, devrons explorer pour construire une informatique où l'utilisateur aura le contrôle de ses données et où la technologie sera au service de l'humain.

22. Le logiciel libre

Le logiciel libre est une condition nécessaire (mais pas suffisante) pour avoir le contrôle et la maîtrise de l'informatique que nous utilisons. En effet, il est possible d'accéder au code du logiciel libre pour l'analyser, l'auditer, comprendre son fonctionnement et finalement se l'approprier en le modifiant si nécessaire. Cette transparence du logiciel libre est garante de la confiance que l'on pourra lui accorder.

À l'inverse, le logiciel propriétaire est une boîte noire : on ne sait pas exactement ce qui est fait par un tel logiciel. L'utilisateur en est réduit à croire sur parole le fournisseur du logiciel, lequel peut avoir introduit dans son produit des portes dérobées, soit pour des raisons mercantiles, soit sous la pression de services de renseignement ; cette opération peut aussi avoir été réalisée par d'autres, à son insu.

Si le logiciel libre est infiniment supérieur au logiciel propriétaire pour ce qui est de la transparence, il a néanmoins d'autres défis à relever, en particulier autour de l'ergonomie et du modèle commercial.

L'expérience utilisateur

Bien trop souvent, les logiciels libres souffrent d'un déficit d'ergonomie. Dans le jargon informatique, on parle d'« expérience utilisateur » (UX, *User Experience*) imparfaite. L'ergonomie n'est pas simplement un problème d'esthétique, mais plutôt de simplicité et d'intuition quand il s'agit d'accomplir une tâche avec le logiciel concerné. Elle doit répondre à des questions qui touchent à la facilité d'usage, à l'évidence de l'interface, au fait que l'utilisateur n'a pas à réfléchir (ou le moins possible) pour se servir de l'outil.

C'est un sujet difficile à aborder pour la plupart des projets de logiciels libres, et ce pour plusieurs raisons.

D'une part, les développeurs de logiciels ont tendance à internaliser le fonctionnement du logiciel sur lequel ils travaillent. Du coup, pour eux, il est évident qu'il faut passer par l'étape 1 avant l'étape 2 puis la 3. C'est normal, ils ont eux-mêmes conçu le logiciel. Ils connaissent son fonctionnement de l'intérieur. Par contre, l'utilisateur final n'a pas cette connaissance intime du produit et de son architecture. Il a donc besoin d'être guidé autant que possible, il a également besoin qu'on ne lui offre pas trop d'options inutiles à chaque étape du processus.

Les développeurs ont souvent un parti pris pour des approches qui sont très efficaces mais qui peuvent rebuter l'utilisateur final. Je prends un exemple : la ligne de commande, ce mode d'interaction avec l'ordinateur qui consiste à taper des commandes dans un « terminal » au lieu de cliquer sur des boutons avec une souris. La ligne de commande peut être formidable de puissance par sa concision. Elle peut aussi être reproduite facilement et programmée dans des scripts. Pour toutes ces raisons, elle est souvent très appréciée des développeurs. Mais voilà, elle rebute l'immense majorité des utilisateurs. C'est une parfaite illustration de ce fossé qu'il faut combler entre développeurs et utilisateurs, faute de quoi l'investissement réalisé par le projet libre pour créer une bonne technologie ne sera pas en mesure de devenir un bon produit capable de rivaliser avec des logiciels propriétaires

concurrents.

Pour cela, il est nécessaire que l'expérience utilisateur soit une préoccupation permanente au sein du projet de logiciel libre, et ce dès le début de ce projet.

Imaginer que l'on puisse voir travailler ensemble des développeurs et des *UX designers* pour faire du logiciel libre n'est pas quelque chose d'impossible. L'expérience utilisateur a par exemple été un grand facteur de différenciation pour le navigateur web Firefox, ce qui lui a permis de concurrencer Internet Explorer. La distribution GNU/Linux Ubuntu a fait de l'ergonomie son cheval de bataille et a été adoptée par des personnes qui n'auraient pas pu, auparavant, utiliser Linux.

Des applications web libres comme l'outil de blog Dotclear 101 et plus récemment, Known 102 ont brillamment démontré que libre et ergonomie n'étaient pas antinomiques. Dans les deux cas, cela a été rendu possible par la collaboration de *UX designers* et de développeurs.

L'épineux problème du modèle d'affaire

L'utilisation de logiciels libres implique une (petite) contrainte pour l'utilisateur : comprendre comment le logiciel en question est financé. Puisque a priori ça n'est pas via la collecte de données personnelles, comment un tel projet peut-il vivre ? Certains projets, comme Dotclear cité plus haut, sont 100 % non lucratifs et reposent sur le travail de bénévoles. Cela peut permettre à un tel logiciel de survivre, pour peu que l'équipe soit motivée. Malgré quelques aléas, Dotclear va bientôt fêter ses quinze ans.

À l'inverse, le projet Wikipédia, qui est un projet libre (d'encyclopédie plutôt que logiciel), a besoin de revenus pour payer l'infrastructure (serveurs, location de data center, connexion à internet) et ses permanents. Pour cela, Wikipédia fait régulièrement des appels aux dons. Cela en fait une encyclopédie gratuite… pour laquelle il faut faire des dons.

De nombreux projets de logiciels libres reposent sur les dons, et il appartient aux utilisateurs de ces logiciels de donner régulièrement pour que les projets soient pérennes. Pour ma part, je donne quelques dizaines d'euros par mois à ces projets. C'est toujours moins que mon abonnement internet, et tout aussi important. Je vous encourage à donner en fonction de vos moyens, mais si tout le monde donnait trois euros par mois, nos logiciels libres seraient bien meilleurs !

23. La maîtrise du serveur

Comment est-il possible d'avoir les fonctionnalités offertes par le *cloud*, notamment la disponibilité permanente et sur plusieurs appareils des applications et de nos données, sans pour autant offrir nos informations à des tiers ?

C'est tout à fait possible, à condition d'avoir la maîtrise du serveur sur lequel tournent ces applications et où sont hébergées nos données.

L'auto-hébergement

On peut imaginer dès aujourd'hui qu'au lieu de mettre toutes nos données chez Google ou auprès de services comme Dropbox (stockage de fichiers), Evernote (stockage de notes), Flickr (partage de photos), on les mette sur des serveurs qui seraient physiquement chez soi, directement connectés à l'ADSL. Comme il s'agit d'un usage individuel, l'ordinateur n'a pas besoin d'être surpuissant, ce qui permet d'avoir recours à des machines à bas coût, consommant très peu d'électricité et ne chauffant quasiment pas. Par exemple, il existe des machines comme le Raspberry Pi 103 qui sont de la taille d'une carte de crédit, valent quelques euros et ne consomment que quelques Watts (compter 70 € environ pour un kit complet avec version haut de gamme, boîtier et alimentation). En connectant une telle machine à un disque dur USB, il est possible de disposer d'un serveur personnel à un prix ridiculement bas.

Par ailleurs, il existe d'ores et déjà dans le commerce une catégorie de produits appelés NAS (*Network-Attached Storage*). Ce sont des boîtiers pouvant accueillir plusieurs disques durs associés à un petit processeur permettant de faire tourner un système d'exploitation et des applications. Certains de ces systèmes fonctionnent avec des logiciels libres.

Les limites de l'auto-hébergement

Il y a quelques obstacles à franchir avant de pouvoir s'auto-héberger. Passons-les en revue.

Le A d'ADSL

L'accès internet haut débit se fait très souvent avec une technologie appelée ADSL, qui signifie *Asymmetric Digital Subscriber Line*. Le souci, c'est le A d'ADSL, qui signifie que le débit des données est asymétrique : les données arrivent vers l'abonné plus vite qu'elles n'en partent. On dit alors que le débit sortant est inférieur au débit entrant. Cela peut-être avantageux dans le cas où on reçoit plus de données qu'on n'en émet, mais c'est un handicap quand il s'agit d'avoir son propre serveur à la maison, qui émet plus qu'il ne reçoit.

Par ailleurs, les fournisseurs d'accès internet ont le plus souvent, dans le contrat qui les lie à leurs abonnés, précisé qu'il était interdit d'héberger un serveur à la maison. À la lumière de ces clauses, on imagine sans peine que le choix de la technologie asymétrique ADSL ne relève pas du hasard et vise plutôt à verrouiller le client dans une position de consommateur.

Cela dit, la fibre optique, technologie bien plus rapide que l'ADSL, commence à se répandre. Et même si elle est également asymétrique, elle permet d'obtenir des débits sortants qui sont tellement importants que cela n'est plus un problème.

L'alimentation électrique

Il est des régions du monde où le courant est moins stable qu'ailleurs. Cela peut être gênant dans la mesure où cela affecte la disponibilité du serveur et de l'équipement réseau.

La sauvegarde des données.

Chaque installation serveur doit disposer d'une procédure de sauvegarde. On peut imaginer une sauvegarde chiffrée envoyée à d'autres systèmes de façon réciproque, chacun ayant une copie chiffrée. De tels systèmes distribués sont en cours de développement, comme par exemple MaidSafe 104.

L'administration du serveur

Les utilisateurs de *cloud* sont habitués à ce que le système fonctionne directement et sans maintenance. En cas de problème, les équipes gérant le *cloud* se chargent de sa résolution. C'est un défi que les solutions libres et décentralisées vont devoir relever : de telles solutions doivent être triviales à administrer pour qu'une grande partie des utilisateurs puisse s'en charger. Cela peut sembler utopique pour l'instant, mais cela n'est pas impossible à réaliser.

24. Le recours au chiffrement

Le chiffrement est une des pierres angulaires du contrôle de nos données. Il permet, en utilisant un secret appelé clé (généralement un mot de passe), d'assurer la confidentialité, l'authenticité et l'intégrité de données, qu'il s'agisse de fichiers ou de messages.

Le chiffrement est essentiel aujourd'hui, car nos différents appareils (PC, smartphone, tablette, serveur) communiquent entre eux via des réseaux interconnectés sur lesquels nous n'avons pas le contrôle : il est possible qu'un tiers écoute nos données pendant qu'elles transitent et cherche à en récupérer une copie, souhaite modifier nos messages ou veuille se faire passer pour quelqu'un qu'il n'est pas.

En ce domaine, les anglicismes sont nombreux, précisons donc un peu de vocabulaire :

Chiffrer : transformer un contenu en clair à l'aide d'une clé (le mot de passe) en un contenu incompréhensible, le contenu chiffré.

Déchiffrer : transformer un contenu chiffré (donc incompréhensible) en contenu en clair à l'aide de la clé.

Décrypter : retrouver le contenu en clair à partir du contenu chiffré sans avoir la clé.

Crypter : ce verbe n'existe pas et ne devrait donc pas être utilisé en français (mais nos amis québécois l'utilisent à la place de chiffrer).

Mot de passe et chiffrement symétrique

L'utilisation d'un mot de passe relève de ce qu'on appelle le chiffrement symétrique. Le mot de passe permet de chiffrer un contenu, et le même mot de passe sera utilisé pour déchiffrer le contenu et le retrouver en clair. Le chiffrement symétrique est très pratique dans certains cas (chiffrer ses fichiers sur son disque dur, par exemple), mais peu pratique dans d'autres cas (par exemple pour envoyer un message à des correspondants). En effet, il faudrait aussi envoyer le mot de passe en clair pour que les destinataires puissent déchiffrer ce que je leur envoie. Un tel mot de passe serait de moins en moins secret et de plus en plus inefficace.

Chiffrement asymétrique : clé privée et clé publique

Le chiffrement asymétrique, appelé aussi cryptographie à clé publique a été inventé à la fin du xxe siècle pour répondre aux limitations du chiffrement symétrique (à mot de passe) expliquées ci-dessus.

Le principe repose sur l'existence de deux clés complémentaires. L'une est publique, connue de tout le monde ; l'autre clé est secrète, connue seulement de son propriétaire.

Le contenu chiffré avec une de ces clés peut être déchiffré par toute personne qui possède l'autre clé, rendant ce chiffrement asymétrique, ce qui est très utile, en particulier dès qu'il s'agit d'envoyer des messages personnels et privés à des tiers.

Ainsi, si Alice veut envoyer un message à Bob, elle prend la clé publique de Bob, qui peut être publiée sur le site web de Bob, par exemple, et chiffre le message avec. Seul Bob, détenteur de la clé privée correspondante, peut déchiffrer le message. Cela permet de préserver la confidentialité du message.

À l'inverse, si Bob chiffre un message avec sa clé privée, il pourra être déchiffré par tous ceux qui ont sa clé publique (qu'il aura pris soin de faire connaître de ses correspondants). On sera donc sûr que ce message a bien été envoyé par Bob. C'est un mécanisme de signature numérique qui permet de s'assurer de l'authenticité d'un message.

Le diable est dans les détails

L'obsolescence des algorithmes de chiffrement

Il existe de nombreux algorithmes de chiffrement, qui sont autant de méthodes possibles pour chiffrer et déchiffrer des contenus. Certaines de ces méthodes sont moins sûres que d'autres : le chiffrement repose sur les mathématiques et les chercheurs de cette discipline font des progrès réguliers, ce qui fait que certains algorithmes autrefois sûrs ne le sont plus aujourd'hui, mais on découvre de nouveaux algorithmes qui sont encore plus solides. Comme pour le conflit entre le serrurier et le monte-en-l'air du monde réel, la technologie progresse tout comme les compétences de ceux qui interceptent les données. Ce qui était sûr hier ne l'est plus autant aujourd'hui.

Chiffrer le contenu ou le tuyau ?

Quand on veut transmettre un message secrètement d'un endroit à l'autre, il y a en gros deux méthodes :

Soit on chiffre le message lui-même, ce qui le rend illisible, et on l'envoie à son destinataire. Peu importe que d'autres l'interceptent en cours de route, son contenu reste incompréhensible. C'est le chiffrement de bout en bout. Soit on ne chiffre pas le message, mais on le transmet par un moyen qui est sécurisé. On peut en effet créer un genre de « tunnel » sécurisé entre un ordinateur et un autre (c'est ce que signifie l'icône du cadenas et le S de https :// dans le navigateur web). C'est le chiffrement de point à point.

Cette distinction entre chiffrement de bout en bout et point à point peut sembler minime, mais elle ne l'est pas. Prenons l'exemple du stockage de mes fichiers dans un service de *cloud*. Si le logiciel que j'utilise chiffre ces données localement avec une clé connue de moi seul, avant d'envoyer ces fichiers sur un serveur distant, je suis le seul à pouvoir lire mes données. Même si un pirate arrive à pénétrer dans le serveur en question ou si les autorités de police en font la demande au service, mes données sont illisibles car chiffrées.

Il arrive que des services de *cloud* promettent la main sur le cœur que nos données sont protégées car chiffrées. Mais en regardant d'un peu plus près, on découvre que seul le transport de ces données est chiffré. En effet, mes fichiers transitent par un « tunnel sécurisé » entre mon ordinateur (ou mon smartphone) et le serveur distant. Mais elles y sont stockées en clair. Autrement dit, les services de police et les éventuels pirates peuvent y accéder sans aucun problème. Et bien sûr, mes données peuvent être analysées par le service de cloud lui-même pour élaborer et améliorer mon profil.

C’est pour cela qu’il faut bien se renseigner avant de choisir de tels services. Le très populaire service de partage de fichiers Dropbox est particulièrement fier de son système : les données sont chiffrées sur mon ordinateur, transitent aussi de façon chiffrée et sont stockées chiffrées sur les serveurs. Pourtant, certaines personnes dont Edward Snowden (le lanceur d’alerte de la NSA) disent clairement : « *il faut abandonner Dropbox* » 105 La raison est toute simple : Dropbox chiffre nos données avec un mot de passe que l’entreprise conserve. Elle peut donc déchiffrer ces données sans même qu’on en soit prévenu.

Conclusion

Le chiffrement peut sembler complexe de prime abord, mais il est essentiel pour protéger notre vie privée et contrer la surveillance de masse.

25. Penser le modèle d'affaire

Une chose est sûre : s'il faut, pour retrouver le contrôle de l'informatique et de nos données personnelles, tendre vers plus de logiciel libre, de chiffrement et d'auto-hébergement, il est un modèle d'affaire qu'il faut fuir : celui de la publicité ciblée.

En effet, la publicité ciblée est ce qui fait que les géants de l'internet vont chercher à tout savoir sur chacun d'entre nous : pour connaître nos centres d'intérêt, nos goûts, nos habitudes, notre pouvoir d'achat et vendre aux annonceurs des espaces publicitaires sur lesquels il y a plus de chance que nous cliquions.

Le souci, c'est que cette concentration de données personnelles et ce profilage rendent économiquement possible la surveillance de masse par les services de renseignement : au lieu d'avoir à pirater des millions de PC pour surveiller tout le monde, il leur suffit de faire des demandes à une poignée de grands acteurs du numérique qui ont déjà fait tout le travail pour eux.

Une solution toute simple (en apparence) existe : payer pour des services qui ne surveillent pas leurs utilisateurs. Comme expliqué au chapitre 15, opérer un service comme Facebook (développement, maintenance, équipements, plus le coût des commerciaux et marketeurs chargés de vendre la publicité) revient à moins de cinq euros par personne et par an, ce qui est moins cher qu'une place de cinéma ou trois cafés. Par an !

La tentation de la gratuité

Curieusement, la gratuité a un attrait disproportionné sur le public, même si cela représente au fond une très mauvaise affaire. Cela tient à un trait de caractère très répandu chez l'humain, décrit par l'économiste comportemental Dan Ariely dans son livre *C'est (vraiment ?) moi qui décide* : « *Quand c'est gratuit, ça fait toujours plaisir. De fait, zéro n'est pas un prix comme les autres, c'est un déclencheur d'émotion — une source d'excitation irrationnelle.* »

Pourtant, si on veut disposer de services respectueux de la vie privée et donc évitant la publicité ciblée, payer ces services avec de l'argent reste la meilleure méthode.

Certains considèrent que la publicité ciblée leur serait plus utile que la publicité normale. Pour ma part, je préfère l'absence de publicité, surtout si c'est pour économiser des sommes aussi réduites.

Il faut savoir qu'il y a des méthodes de personnalisation de la publicité qui ne passent pas par la collecte de données par les grands acteurs d'internet. Il existe par exemple la notion de « Gestion de la relation vendeur » (en anglais *Vendor Relationship Management* – VRM) telle que pensée par Doc Searls dans son projet VRM 106 développé à l'université d'Harvard. Le principe consiste à donner aux consommateurs des outils qui font deux choses :

- donner de l'indépendance aux individus face aux grandes entreprises qui les pistent et les enferment dans leurs services ;
- offrir aux consommateurs de meilleurs moyens pour qu'ils communiquent aux vendeurs ce qu'ils

recherchent.

Suivant le principe du VRM, un consommateur peut décider ce qui l'intéresse. Si j'envisage d'acheter une moto à court ou moyen terme et que je m'intéresse à la musique Rock et au Rugby, je devrais pouvoir l'indiquer quelque part (probablement dans mon navigateur web) pour que les publicités s'adaptent en fonction de mes goûts et besoins, sans avoir à être traqué pour autant.

En attendant que le principe du VRM permette une publicité respectueuse de l'utilisateur, il va nous falloir réapprendre à payer les services que l'on utilise au lieu d'échanger bêtement nos données personnelles contre des outils qui ne coûtent presque rien. À ce propos, je laisse la conclusion à John Naughton qui tient une chronique au *Guardian* 107 :

Quand viendra le temps où l'on écrira l'histoire de l'époque actuelle, nos arrière-petits-enfants s'étonneront d'apprendre que des milliards de gens apparemment sains d'esprit ont accepté passivement ce marché lamentablement déséquilibré. (Ils se demanderont aussi sûrement pourquoi nos gouvernements n'ont porté à cette histoire qu'un intérêt très limité).

26. Faire mieux que les systèmes centralisés

Si l'on construit des outils nous permettant d'avoir le contrôle sur nos données, des SIRCUS, il ne suffira pas qu'ils respectent les quatre principes traités dans les chapitres précédents (logiciel libre, auto-hébergement, utilisation du chiffrement et indépendance vis-à-vis de la publicité ciblée). Il faut également qu'ils aient du succès, qu'ils soient adoptés massivement et remplacent petit à petit les solutions actuelles, faute de quoi ils ne pourront pas renverser les tendances à la centralisation et au profilage, qui mènent à la surveillance de masse.

Pour assurer le succès des SIRCUS, trois critères supplémentaires doivent être remplis : ergonomie, interopérabilité et plus-value pour l'utilisateur.

Intégrer ergonomie et chiffrement dès le départ

J'ai longuement abordé le sujet de l'ergonomie dans le chapitre sur le logiciel libre de cette troisième partie, je ne vais pas m'étendre beaucoup plus. Il convient juste de se souvenir que le logiciel doit être écrit pour l'utilisateur et non pas pour son concepteur. Son utilisation doit être évidente et plaisante, ce qui rend cependant les choses plus compliquées pour les développeurs : ce qui est simple à utiliser est bien souvent complexe à construire.

Le défi est particulièrement grand dans la mesure où le respect de la vie privée, donc le besoin d'une architecture distribuée et reposant sur le chiffrement, ajoute des contraintes supplémentaires qui ont des impacts sur l'expérience utilisateur.

Les logiciels intégrant de la cryptographie sont parfois très complexes à utiliser, et les logiciels libres n'y font pas exception ; j'en veux pour preuve le chiffrement d'emails dans Thunderbird avec l'extension Enigmail et GPG, avec lesquels j'ai encore des soucis à l'heure où j'écris ces lignes.

Ce n'est pas toujours le cas : l'utilisation du protocole web https:// (qui permet d'accéder à des sites web de manière sécurisée) est très généralement transparente. Elle ne devient compliquée que lorsqu'on a affaire à des certificats auto-signés, mais ce problème est en passe d'être résolu avec des initiatives comme Let's Encrypt. Let's Encrypt 108 est une autorité de certification ouverte, distribuée et sécurisée, soutenue par de très nombreux acteurs de l'internet, qui n'est réellement publique que depuis avril 2016, mais devrait grandement révolutionner le marché abusif de la sécurité et de la vente de certificats, tel qu'il existe aujourd'hui.

Interopérabilité

Sous ce nom un peu barbare se cache une idée toute simple : être interopérable, c'est être compatible avec les produits existants et à venir.

Wikipédia en donne une définition un peu plus élaborée 109 :

L'interopérabilité est la capacité que possède un produit ou un système, dont les interfaces sont intégralement connues, à fonctionner avec d'autres produits ou systèmes existants ou futurs et ce sans

restriction d'accès ou de mise en œuvre.

L'interopérabilité est nécessaire car l'informatique évolue sans cesse, et il est important de pouvoir quitter une solution pour une autre si le besoin s'en fait sentir. Cela peut se faire simplement pour certaines applications comme la sauvegarde de fichiers ou la gestion des contacts (il existe des standards pour cela). Cela peut être plus compliqué dans les cas où on utilise des applications plus complexes pour lesquelles aucun standard n'a été créé, comme par exemple un outil de gestion de blog où, à ma connaissance, la seule façon de migrer repose sur l'utilisation d'une « moulinette » *ad hoc* qui lit les données dans un format pour les écrire dans un autre format.

Interopérabilité et médias sociaux

Dès lors que l'on touche aux fonctionnalités sociales des applications, l'interopérabilité se complexifie encore plus. Si la migration d'un système de stockage fichiers dans le *cloud* centralisé vers un autre décentralisé ne concerne que l'utilisateur propriétaire des fichiers, le problème est autrement plus compliqué dès qu'il s'agit d'arrêter de publier sur Facebook pour publier sur son propre blog : le web social, par essence, touche un utilisateur et tous ses contacts.

Pour convaincre, l'approche SIRCUS ne peut pas se permettre de demander aux nouveaux utilisateurs de choisir entre interactions sociales et respect de la vie privée.

Il devient donc nécessaire de promouvoir l'interopérabilité des fonctionnalités sociales, et d'imposer le respect des normes afférentes aux grandes plateformes. Il existe en ce domaine deux initiatives intéressantes.

SocialWeb du W3C

Le W3C, l'organisme qui produit les normes du web, a publié des travaux sur un « w *eb social ouvert, respectueux de la vie privée et reposant sur les normes* » 110. Sans rentrer dans les détails, car cela sortirait de l'objectif du présent ouvrage, ce document aborde nombre des problèmes rencontrés par les utilisateurs sur les réseaux sociaux :

- portabilité des données d'un système à l'autre ;
- identité ;
- capacité à faire des liens d'un réseau à l'autre ;
- vie privée.

IndieWebCamp

IndieWebCamp 111 est une autre initiative sur un sujet comparable, mais menée d'une manière très différente, par des gens qui ont eux aussi été souvent impliqués dans les standards du web.

L'approche d'IndieWebCamp repose sur la décentralisation (que chacun possède son propre site avec son propre nom de domaine), le contrôle des contenus partagés et l'interfaçage avec les grands réseaux sociaux.

Parmi les concepts poussés par IndieWebCamp, POSSE 112 est l'un des plus intéressants. POSSE signifie « *Publish On your Own Site, Syndicate Elsewhere* » (Publiez sur votre propre site, diffusez

ailleurs). Dans ce modèle, l'utilisateur publie une photo sur son site personnel, qui le diffuse alors sur les médias sociaux de son choix, comme Flickr (site de partage de photos) ou Facebook. De même, un billet de blog sera publié sur le site personnel et relayé sur les autres grands réseaux sociaux.

À chaque fois, les commentaires et réactions à ces publications sur les réseaux sociaux seront copiés sur le site personnel. Ainsi, le jour où l'utilisateur souhaitera quitter Facebook, il ne perdra pas ses photos, ses interactions, ses articles et autres.

Ce qui est peut-être le plus important dans l'approche POSSE, c'est qu'un utilisateur peut décider d'avoir son propre site indépendant pour reprendre le contrôle de ses données, tout en continuant à interagir avec ses contacts, en bénéficiant de l'audience des grands réseaux sociaux centralisés. Ainsi, il n'est pas nécessaire de choisir entre contrôle de nos données et interactions sociales. C'est une excellente nouvelle car un tel choix serait nécessairement défavorable aux approches décentralisées.

Offrir une plus-value immédiate à l'utilisateur

Soyons lucides : à part une petite frange de *geeks*, rares sont les utilisateurs qui ont envie de changer leurs habitudes informatiques. Peur du changement, de l'inconnu, de perdre un système qu'ils ont eu du mal à faire fonctionner, les utilisateurs sont rarement téméraires quand il s'agit de changer d'ordinateur et de logiciels.

C'est pourquoi, si on veut toucher les utilisateurs au-delà du cercle restreint des libristes militants (dont je fais partie), si on veut les convaincre de passer d'un modèle centralisé à un modèle SIRCUS respectueux de leurs données et de leur vie privée, il va falloir offrir une véritable plus-value.

Mauvaise nouvelle : le contrôle des données, le respect de la vie privée ne sont pas suffisants, et ce pour une raison toute simple : ils ne sont pas tangibles ; il est très difficile de voir, de ressentir, que d'un côté on contrôle nos données et que de l'autre notre vie privée est mieux protégée. La preuve, les gens ont mis des années à comprendre qu'elle ne l'était pas quand ils sont passés sur Facebook.

Pour donner envie à un utilisateur de passer au modèle SIRCUS, il faut lui donner un avantage tangible, désirable et immédiat.

Offrir une expérience utilisateur comparable à celle de Google, de Facebook ou de Dropbox n'est pas suffisant : l'effort à fournir pour passer du modèle centralisé à l'approche SIRCUS est beaucoup trop élevé pour l'utilisateur moyen. Pour le convaincre, il faut lui offrir un « moment Ahah », un moment où il se dira « Ah oui, c'est génial ce truc, je n'aurais pas pu le faire avec Facebook ou Google ». Les Américains appellent cela la *killer feature*, la fonctionnalité qui tue.

Tout le défi pour ceux veulent construire des offres SIRCUS se trouve là… trouver l'application majeure. Car il en reste encore à découvrir !

Notes

100 « Surveillance is the Business Model of the Internet: Bruce Schneier » (La surveillance, c'est le Business Model de l'Internet), Bruce Schneier, *Security Week*, 9 avril 2014 – http://www.securityweek.com/surveillance-business-model-internet-bruce-schneier.

101 http://fr.dotclear.org/.

102 Known, « un seul site pour tout le contenu que vous créez » – https://withknown.com/.

103 La Raspberry Pi Foundation a vendu plus de cinq millions d'unités – https://www.raspberrypi.org/.

104 Système SAFE (Secure Access For Everyone) – http://maidsafe.net/.

105 « Dropbox : Edward Snowden en déconseille l'utilisation », *ZDNet*, 18 juillet 2014 – http://www.zdnet.fr/actualites/dropbox-edward-snowden-en-deconseille-l-utilisation-39804029.htm.

106 « ProjectVRM seeks to improve markets by equipping customers with tools for both independence from vendors and better engagement with vendors » (Le projet VRM vise à améliorer les marchés en équipant les clients avec des outils leur donnant une plus grande indépendance vis-à-vis des fournisseurs tout en dialoguant mieux avec ces derniers – https://cyber.law.harvard.edu/research/projectvrm.

107 « Fightback against internet giants' stranglehold on personal data starts here » (La revanche contre la mainmise des géants de l'Internet sur les données personnelles commence), John Naughton, *The Guardian*, 1er février 2015 – http://www.theguardian.com/technology/2015/feb/01/control-personal-data-databox-end-user-agreement.

108 https://letsencrypt.org.

109 Interopérabilité, Wikipédia – https://fr.wikipedia.org/wiki/Interop%C3%A9rabilit%C3%A9.

110 « A Standards-based, Open and Privacy-aware Social Web » (Un web social ouvert, appuyé sur des normes et conscient de la vie privée) – *W3C* https://www.w3.org/2005/Incubator/socialweb/XGR-socialweb-20101206/.

111 « IndieWeb est une alternative aux entreprises du web commercial, focalisée sur les gens » – https://indiewebcamp.com/.

112 POSSE – http://indiewebcamp.com/POSSE.

Partie IV

Un internaute averti en vaut dix

Limiter la surveillance au quotidien

Partie IV
Un internaute averti en vaut dix

Limiter la surveillance au quotidien

27. Partir sur de bonnes bases

Dans cettequatrième partie, nous allons passer à l'action. Ce passage à l'action est pour moi essentiel. En effet, si vous avez ce livre entre les mains, c'est que le sujet de la vie privée et de la surveillance de masse vous préoccupe. Mais, dans la grande majorité des cas, nous ne savons pas comment faire pour nous en protéger. Du coup, on se résigne à subir, et on reste passif. Or, il est possible de passer à l'action, de commencer à faire quelque chose. C'est l'enjeu des chapitres suivants.

Que veut-on protéger et contre quoi ?

En sécurité informatique existe la notion de « modèle de menace » (*threat model*), qui désigne ce que l'on veut protéger et ce dont on veut se protéger.

Dans le cas présent, je pars du principe que nous voulons protéger l'équipement et les services qu'est susceptible d'utiliser un particulier : un ordinateur, un smartphone, une tablette, et les quelques services du *cloud* qu'il utilise. Contre quoi veut-on se protéger ? Contre la maximisation de la collecte de données personnelles. On veut limiter la fuite de ses données personnelles, pas l'empêcher complètement. Ce serait louable, bien sûr, mais cela rendrait la tâche trop complexe et trop contraignante.

Les choses sont claires : je n'ai pas la prétention de permettre au lecteur de devenir invisible ou anonyme sur internet. Je pense d'ailleurs que cela demande trop d'efforts, ce qui fait que personne ou presque n'est prêt à cela, à part les gens comme Edward Snowden dont la vie dépend du fait qu'on ne sache pas où le retrouver. Autrement dit, si vous êtes un blogueur, un journaliste ou un dissident dans une dictature, ou si vous êtes apprenti-terroriste et que vous voulez vous protéger contre toute surveillance informatique possible, vous n'êtes pas en train de lire ce qu'il faut 113.

Par contre, il y a un certain nombre de mesures qu'il est possible de mettre en œuvre dès maintenant, sans grandes connaissances en informatique et qui n'imposent pas de changer trop ses habitudes. C'est ce que nous allons passer en revue, en démontrant qu'agir est possible, avec l'espoir que cela encouragera le lecteur à se renseigner pour aller plus loin. Mon objectif ici est à la fois modeste et très ambitieux. Modeste, car il vise à indiquer comment commencer à se protéger. Ambitieux, car cela signifie que l'on sort de la posture de l'utilisateur qui ne sait pas se protéger et se résigne à offrir ses données aux spécialistes. Commencer à se protéger, c'est agir, c'est arrêter de subir. Prêt ? C'est parti !

Système d'exploitation

Le système d'exploitation, c'est le logiciel de base qui permet de faire tourner les applications. La plupart des gens utilisent Windows, d'autres OSX (sur les Mac) et d'autres enfin GNU/Linux (souvent sous la marque Ubuntu).

Chaque système d'exploitation a ses avantages et ses inconvénients, et surtout nous avons tous nos habitudes, donc je vais bien me garder de vous recommander l'un ou l'autre 114.

Une chose est sûre toutefois : il faut avoir un système d'exploitation tenu à jour. En effet, les systèmes d'exploitation étant des choses très complexes faites par des humains, ils comportent des défauts (des bugs), dont certains peuvent être exploités par des personnes mal intentionnées pour pénétrer dans votre ordinateur. Un bug permettant cela est appelé une « faille de sécurité ».

Les correctifs de bugs sont souvent distribués aux utilisateurs sous forme de *patchs* (rustines, en français) par Microsoft, Apple et les distributions Linux. Il est très important de mettre à jour votre système d'exploitation en appliquant ces *patchs* chaque fois que votre machine vous le propose.

Attention : les sociétés fournissant les systèmes d'exploitation (Microsoft, Apple, etc.) cessent de fournir des *patchs* au bout d'un certain temps. Aussi, Windows XP et Mac OSX 10.7-Lion ne sont plus maintenus. Des trous de sécurité existent dans ces systèmes, qui seront découverts demain… mais ne recevront jamais de correctifs. Il est donc très important de passer à une version plus récente et encore maintenue du système d'exploitation que vous avez choisi. On notera que cela signifie parfois qu'il faut changer l'ordinateur pour cela, puisque dans certains cas les nouveaux systèmes d'exploitation ne peuvent pas tourner correctement sur d'anciennes machines, devenues obsolètes et non prises en compte. Cela fait malheureusement partie de l'obsolescence programmée, mise en place cyniquement pour vendre toujours plus de matériel informatique.

Antivirus

Il existe des logiciels appelés virus, qui se dupliquent de machines en machines. Ces virus sont dangereux, soit parce qu'ils sont faits pour nuire (destruction de données), soit pour prendre nos données en otage (les données sont verrouillées et il faut payer pour y avoir accès – on parle alors de *ransomware*, qui demandent une rançon pour libérer vos propres données), soit ces virus ralentissent nos machines en leur faisant exécuter des tâches mystérieuses. Dans tous les cas, il faut s'en protéger.

À l'heure actuelle, les virus touchent principalement les machines Windows.

Pour se protéger des virus, il faut installer un antivirus. De nombreux antivirus gratuits existent pour les différentes versions de Windows, mais tous ne se valent pas. L'antivirus gratuit le plus populaire en ce moment est Avast 115, mais les offres payantes sont nombreuses et souvent efficaces. On notera que, comme tous les logiciels, l'antivirus doit être maintenu à jour pour que ses bugs soient corrigés et qu'il puisse détecter les nouveaux virus.

Si on décide d'installer Avast, il faut se souvenir que c'est un produit gratuit proposé par une société commerciale, aussi convient-il de se méfier. Ainsi, lors de l'installation, sur le premier écran, il faut décocher les cases « Installer le navigateur Google Chrome » et « Faire de Google Chrome mon navigateur par défaut » qui sont affichées en gris sur fond gris. En effet, Google finance Avast pour que celui-ci diffuse le logiciel Chrome (nous verrons pourquoi au chapitre suivant).

Ensuite, il faut bien lire et décoder l'avertissement affiché sur le deuxième écran de l'assistant d'installation d'Avast. En effet, même si ses auteurs promettent de protéger notre vie privée, plus loin dans le texte, on peut lire :

Nous utilisons effectivement les informations que nous recueillons […] ces informations peuvent être partagées par des tierces parties en dehors d'Avast.[…]Si, après avoir installé le produit, vous préférez ne pas participer à cette collecte de données, vous pouvez la refuser ultérieurement en changeant cette option dans les paramètres.

Pour cela, à la fin de l'installation d'Avast :

Cliquer sur le bouton « Paramètres » (représenté par un engrenage). Il est en bas à gauche de la fenêtre d'installation.

Faire défiler les options vers le bas en cherchant la section « Confidentialité ».

Cliquer sur « Confidentialité » pour révéler les options.

Décocher la case « *Participate in data sharing* ».

Cliquer sur OK pour valider.

Voilà, Avast est installé et il est réglé pour être le moins intrusif possible envers votre vie privée.

Sauvegarde

Nos machines stockent nos données sur des disques durs qui, comme toutes les machines, sont susceptibles de tomber en panne ou d'être détruits accidentellement. Pour éviter de perdre nos données, il faut en faire régulièrement une copie de sauvegarde. Cette copie peut être faite sur un DVD vierge ou, mieux, un disque dur externe qu'il faut se procurer. On en trouve à partir d'une soixantaine d'euros pour 500 Go à 1 To d'espace.

Depuis Windows 7, des outils permettant de faire facilement des sauvegardes sont intégrés au système :

Une fois le disque dur branché, aller dans le menu démarrer.

Cliquer sur « Système et sécurité » puis « Sauvegarder et restaurer ».

Cliquer enfin sur « Configurer la sauvegarde » et suivre les instructions.

Pour un Mac, il faut brancher le disque dur externe puis suivre les instructions proposant d'utiliser la fonctionnalité « Time Machine ».

Pour Linux, il existe de nombreuses solutions, qui sont pour la plupart dans l'aide de la distribution Ubuntu 116. Elles vont de l'incontournable rsync, en ligne de commande, jusqu'à Déjà Dup, une interface graphique qui pilote le logiciel Duplicity, qui lui-même repose… sur rsync.

Chiffrement du disque

Dans le cas où vous utilisez un ordinateur portable en déplacement, il n'est pas exclu qu'il soit volé, perdu ou oublié. Pour éviter que les données soient exploitées par la personne le récupérant, il est recommandé de chiffrer son disque dur.

À cet effet, certaines versions de Windows intègrent un logiciel appelé BitLocker qu'il faudra utiliser.

Sur Mac, c'est l'option FileVault qui offre cette possibilité de chiffrer son disque dur. L'activation de FileVault peut se faire à la première utilisation du Mac. Si vous n'avez pas activé cette option, il est

possible de le faire à tout moment. Pour cela :

Sélectionner « Sécurité et Confidentialité » dans les préférences système (accessibles depuis le menu Pomme).

Cliquer sur FileVault. Cliquer sur le cadenas pour déverrouiller les options, cliquer sur « Activer FileVault » et suivre les instructions.

Le chiffrement sur Ubuntu Linux est possible sans rien installer lorsqu'on crée un utilisateur. Cela ne chiffre que le répertoire de cet utilisateur et repose sur le paquet ecryptfs-utils, mais cela peut s'avérer suffisant pour la plupart des cas. Si l'on souhaite un maximum de sécurité, on pourra avoir recours au chiffrement de tout le disque via dm-cryptet LVM.

Et maintenant ?

Voilà, nous avons fait le tour des choses importantes à mettre en œuvre pour être un peu plus en sécurité. Un système d'exploitation à jour, un antivirus, une sauvegarde (à effectuer régulièrement !) et cerise sur le gâteau, le chiffrement du disque dur. Voyons maintenant ce que l'on peut faire au niveau du navigateur web.

28. Choisir et personnaliser son navigateur

Le navigateur est une application particulièrement importante de nos jours, dans la mesure où il permet d'utiliser les sites web, qui bien souvent captent nos données. Voyons comment faire pour continuer à utiliser internet dans de bonnes conditions tout en préservant le contrôle de nos données.

Choix du navigateur

Tout d'abord, il faut choisir un navigateur qui soit digne de confiance. On peut d'ores et déjà éliminer Google Chrome, qui est proposé par Google et utilisé par celui-ci pour capturer nos données. De manière générale, les navigateurs proposés gratuitement par des sociétés commerciales dont le modèle d'affaire est la publicité ciblée (Google, Opera [117]) sont à éviter pour des raisons évidentes. Il reste donc ces options :

Firefox de Mozilla. Un logiciel libre fourni par une organisation à but non lucratif – https://www.mozilla.org/fr/firefox/.

Safari d'Apple. Logiciel non libre fourni par une société commerciale mais dont le revenu vient de la vente de matériel. Livré avec les matériels Apple, et seulement disponible pour eux. Côté fonctionnalités, il est en net retrait par rapport à Chromium et Firefox.

Chromium, une variante libre de Google Chrome, débarrassé des modules qui envoient vos données à Google. Le souci avec Chromium, c'est que Google, qui en est responsable, n'a pas intérêt à le promouvoir, et donc limite les mises à jour automatiques, ce qui fait que je ne peux pas le recommander à l'internaute ordinaire.

Internet Explorer (IE) de Microsoft, logiciel propriétaire. Même si Microsoft possède une branche consacrée à la publicité ciblée, IE ne semble pas collecter trop d'informations sur l'utilisateur. Mais même s'il a fait des progrès en termes d'ergonomie et de fonctionnalités, ce navigateur est moins efficace que les trois autres. Internet Explorer est en passe d'être remplacé par Edge, un nouveau navigateur produit par Microsoft. Edge ne fonctionne que sur Windows 10 et vient de sortir alors que j'écris ces lignes. La nouvelle politique de Microsoft quant à la récupération croissante de données personnelles, combinée au fait que je n'ai pas encore pu le tester, m'empêche de le recommander.

Cela fait 17 ans que je contribue au projet Mozilla et j'ai bien sûr choisi d'utiliser Firefox à titre personnel, en plus du fait que c'est un logiciel libre et qu'il est fait par une organisation dans laquelle j'ai confiance. Aussi, pour la suite de ce chapitre, même si les quatre navigateurs cités ci-dessus sont de qualité, je prendrai le cas de Firefox pour mes exemples. Souvent, des fonctionnalités du même type existent pour les autres navigateurs, mais avec des noms différents.

Prendre de bonnes habitudes

Télécharger le navigateur depuis le site officiel

C’est un fait, de nombreux sites non-officiels récupèrent des logiciels populaires et les proposent au téléchargement. Mais cela n’est pas par pure bonté d’âme… Bien souvent ces sites ajoutent des *malwares* ou des *crapwares*, des logiciels non-désirés et parfois dangereux (virus, etc.). Aussi, pour télécharger un logiciel, il faut toujours se rendre sur le site officiel. Dans le cas de Firefox, il faut utiliser le navigateur déjà installé sur votre machine (Internet Explorer pour une machine Windows, Safari pour un Mac) et visiter la page web https://www.mozilla.org/fr/firefox/puis cliquer sur le bouton « téléchargement gratuit ». À l’installation, il est recommandé de choisir Firefox comme navigateur par défaut.

Maintenir son navigateur à jour

Les logiciels sont des systèmes très complexes, surtout les navigateurs. Aussi, sont-ils constamment améliorés : on leur rajoute de nouvelles fonctionnalités, on corrige leurs défauts dont certains sont susceptibles de poser des problèmes de sécurité et pourraient permettre à des personnes mal intentionnées, des « pirates », d’avoir accès à vos données. De ce fait, il est très important de mettre à jour le navigateur dès qu’il le propose. Dans Firefox, un système de mise à jour automatique télécharge les nouvelles versions en arrière-plan. Il suffit d’accepter la mise à jour quand Firefox la propose pour être mieux protégé.

De même, un logiciel complémentaire comme Flash est parfois nécessaire pour certains sites. Il faut le télécharger depuis le site officiel 118 et le maintenir à jour.

Utiliser un mot de passe principal

Il est vivement recommandé d’avoir des mots de passe différents d’un service à l’autre. En effet, il arrive que les mots de passe soient compromis, c’est-à-dire que des personnes mal intentionnées en prennent connaissance. Si vous n’utilisez qu’un seul mot de passe pour tous les services, un pirate ayant récupéré le mot de passe peut accéder à tous vos comptes, ce qui lui permet d’usurper votre identité, avec des conséquences potentiellement désastreuses. Pour éviter cela, il faut idéalement utiliser des mots de passe complexes (donc difficiles à deviner) différents pour chaque service. Comme cette complexité rend la mémorisation difficile, il existe dans Firefox un gestionnaire de mot de passe, qui enregistre les différents mots de passe et les saisit pour vous quand c’est nécessaire. C’est très pratique, mais pour plus de sécurité, il est recommandé de les protéger à leur tour… par un mot de passe principal. Pour cela :

Aller dans les préférences de Firefox (Mac : menu Firefox puis Préférences. Windows : appuyer sur la touche ALT pour faire apparaître la barre de menus, puis menu Outils et choisir Options).

Une fois dans la boîte de dialogue, sélectionner le cadenas « Sécurité », cocher la case « Utiliser un mot de passe principal », saisir deux fois un mot de passe que vous retiendrez. C’est le seul que vous devrez retenir, il vous sera demandé à chaque fois que vous redémarrerez Firefox. Il sert à verrouiller le gestionnaire de mots de passe.

Choisir les bonnes extensions

Firefox a popularisé le système des extensions pour navigateurs. Ces extensions permettent de personnaliser le navigateur. J'en ai sélectionné plusieurs qui aident à la sécurité et limitent le pistage des utilisateurs.

HTTPSeverywhere

Certains sites communiquent avec leurs utilisateurs de façon chiffrée (httpS ://), d'autres de façon non-chiffrée (http ://). Certains offrent les deux possibilités. HTTPSeverywhere choisit automatiquement de communiquer de façon chiffrée quand c'est possible. Cela augmente la sécurité.

Il est très simple de l'installer depuis : https://www.eff.org/Https-everywhere. Attention : Firefox décourage l'installation d'extensions provenant de sites autres que le site officiel des extensions Firefox, il faut donc cliquer sur le bouton « accepter ». Au passage, il faut remarquer que cela doit être fait de façon exceptionnelle car, pour des raisons de sécurité, il vaut mieux éviter d'installer des extensions Firefox provenant de sites autres que le site officiel de Mozilla, https://addons.mozilla.org.

Installer un anti-mouchard

Il existe de nombreux sites publicitaires qui nous pistent au quotidien grâce à des mouchards cachés dans les pages web. Certaines extensions, que l'on pourrait appeler des « anti-mouchards » peuvent bloquer ces mouchards. J'ai longuement testé les extensions Ghostery et Privacy Badger. J'avais un a priori favorable pour Privacy Badger car c'est un logiciel libre alors que le code source de Ghostery n'est pas libre. Pourtant, mon impression est que Ghostery ne ralentit pas ma machine par opposition à Privacy Badger. Aussi, je vais détailler comment installer Ghostery, même si son paramétrage est plus complexe que celui de son alternative.

On peut installer Ghostery depuis le site des extensions Firefox, https:// addons.mozilla.org. Cette extension se décrit ainsi :

Ghostery recherche les éléments de page tiers (ou « mouchards ») présents sur les pages web que vous visitez. Il peut s'agir de *widgets* pour les réseaux sociaux, de publicités, de pixels invisibles utilisés pour le suivi et l'analyse, etc. Ghostery vous informe de leur présence et vous indique les entreprises qui en sont à l'origine. Vous pouvez en savoir plus sur ces entreprises et, si vous le souhaitez, bloquer leurs mouchards.

Juste après l'installation, on passe par une série de panneaux successifs permettant d'affiner les paramètres. Je recommande de bloquer les éléments suivants :

> Analytique – ce sont les mouchards visant à mesurer l'audience des sites web.
>
> Balises – comparable à Analytique, mais avec une technologie différente.
>
> Confidentialité.
>
> Publicité – publicité ciblée.
>
> *Widgets* – module provenant d'un site tiers mais offrant des fonctionnalités (ajout de commentaire, partage vers des réseaux sociaux etc.).

La neutralisation des *widgets* ferait perdre des fonctionnalités dans les sites, laissant l'impression que

certaines pages ne fonctionnent pas bien. Aussi je ne recommande pas de les désactiver.

Voici le paramétrage que je recommande :

Ne pas activer Ghostrank.

Désactiver les infobulles d'alerte.

Cocher les cases Analytique, Balises, Confidentialité et Publicité. Laisser la case *Widgets* décochée.

Aller ensuite dans l'onglet « Cookies ».

Faire de même que dans l'onglet précédent et cocher Analytique, Balises, Confidentialité et Publicité. Laisser la case *Widgets* décochée.

Passer au dernier panneau de l'assistant.

Et voilà, Ghostery est installé !

Utiliser un moteur de recherche plus respectueux de la vie privée

La recherche sur le web est une activité importante pour chacun, mais c'est aussi celle qui est la plus révélatrice de nos préoccupations, dans la mesure où l'on communique directement au moteur de recherche ce qui nous préoccupe et nous questionne. Nul besoin pour autant de passer par la recherche Google comme neuf Français sur dix. Il existe en effet plusieurs services alternatifs. Tous étant gratuits, il convient de comprendre leurs modèles de revenus et se méfier de l'omniprésente publicité ciblée.

Les services non-commerciaux

Le moteur de recherche en logiciel libre Searx a une approche intéressante : comme Google, il demande à l'utilisateur des mots-clés, mais il transmet cette recherche à plusieurs moteurs traditionnels commerciaux puis fusionne les réponses de chacun avant de les présenter à l'utilisateur. En jouant ce rôle d'intermédiaire entre l'utilisateur et les différents moteurs commerciaux, il anonymise la connexion, ce qui évite le pistage. Il y a deux inconvénients majeurs à cette approche. La première est la rapidité de la réponse. On multiplie les intermédiaires, donc le traitement est plus long, et la réponse n'est affichée sur la machine de l'utilisateur que lorsque tous les moteurs ont fini d'envoyer leurs réponses respectives. Au final, l'affichage se fait attendre quelques secondes, ce qui peut paraître une éternité dans notre monde moderne. L'autre inconvénient est lié au modèle d'affaire. Sans affichage publicitaire, il n'y a pas de revenu pour le site qui fait fonctionner le logiciel Searx. Certaines associations très en pointe pour la défense de nos droits et de la vie privée, comme La Quadrature du Net et Framasoft, opèrent un service Searx. Si vous aimez leurs services (respectivement sur https://searx.laquadrature.net/e t https://framabee.org/), je vous encourage vivement à faire un don à ces associations pour payer les frais de fonctionnement de ces services.

Les services commerciaux

Les trois principaux acteurs commerciaux revendiquant le respect de la vie privée sont Qwant

(français), DuckDuckGo (américain) et Startpage (néerlandais). Qwant utilise sa propre technologie, là ou les deux autres utilisent les résultats de Google, ce qui limite l'émergence d'une alternative, mais protège l'utilisateur du profilage.

Le modèle commercial de Qwant repose sur l'affiliation (si on cherche un objet dans Qwant et qu'on l'achète dans la foulée sur un site marchand, le moteur est rémunéré par le site marchand). Les deux autres affichent de la publicité en fonction des mots-clés de la recherche. À l'usage, Qwant semble plus pertinent que les deux autres pour les recherches en langue française.

Pour ces raisons, je recommande l'utilisation de Qwant. Pour l'installer et en faire votre moteur de recherche par défaut, procédez ainsi :

Aller sur le site https://qwant.com.

Cliquer sur la loupe dans le champ de recherche (en haut à droite de la fenêtre Firefox).

Cliquer sur « Ajouter Qwant ».

Cliquer à nouveau sur la loupe puis sur « Modifier les paramètres de recherche ». Une fenêtre s'ouvre.

Sélectionner Qwant comme moteur de recherche par défaut.

Voilà, vos prochains résultats de recherche sur le web seront fournis par Qwant, dans le respect de votre vie privée !

Faut-il bloquer les publicités ?

Certains vous recommanderont de bloquer la publicité dans votre navigateur. Il est vrai que cela peut augmenter la rapidité de chargement des pages et encourage une navigation plus sereine car dépourvue de ce qui est souvent une pollution visuelle.

Pourtant j'ai décidé de ne pas bloquer la publicité dans mon Firefox. En effet, la publicité est la principale si ce n'est l'unique façon pour l'immense majorité des sites web de se rémunérer. En bloquant la publicité, j'ai le bénéfice à court terme d'une navigation plus rapide et avec moins de distractions, mais à moyen et long terme, les sites n'auront plus les moyens de publier du contenu original et de qualité. C'est d'autant plus gênant que l'histoire prouve que la presse indépendante est une condition essentielle pour avoir une démocratie en bonne santé… et ni notre presse, ni notre démocratie, ne sont actuellement en bonne santé. Évitons donc d'empirer les choses.

Si vous le souhaitez, vous pouvez installer un bloqueur de pub (souvent appelé *Adblocker*), mais je pense que ce n'est pas une bonne idée, d'autant plus que l'extension vedette, AdBlockPlus, consomme beaucoup de mémoire et accepte de l'argent de certains annonceurs pour laisser apparaître leurs publicités, une pratique que d'aucuns considèrent comme mafieuse. Si vous souhaitez néanmoins utiliser un bloqueur, je vous recommande plutôt l'extension uBlock Origin [119].

Il est toutefois un type particulier de publicité que je bloque : celles à base de Flash (elles jouent de la vidéo et de la musique et consomment beaucoup d'électricité, réduisant du coup l'autonomie de ma batterie). Pour bloquer Flash, j'utilise l'extension Flashblock [120], en attendant le moment que j'espère proche où le recours à Flash sera totalement inutile [121].

Le mode Navigation privée

Il existe une fonctionnalité des navigateurs qui s'appelle « navigation privée », qui est fort mal nommée. Certains recommandent son utilisation au quotidien, mais je trouve pour ma part qu'elle est contre-productive. Explications.

Il faut savoir que chaque navigateur, qu'il s'agisse de Firefox ou des autres, conserve un historique de navigation sur votre PC. Cela permet de retrouver ultérieurement et plus facilement une page déjà visitée. Ainsi, quand je tape la lettre « m » dans la barre d'adresse, Firefox me propose immédiatement de visiter la page http://www.meteofrance.com/accueil, car c'est une page que je consulte souvent pour savoir si je dois emporter ma combinaison de pluie lors de ma prochaine sortie moto [122].

Le mode navigation privée fait que Firefox ne va pas mémoriser l'historique de mes différentes visites sur les sites web. Cette information n'est normalement pas partagée avec des tiers (sauf cas très particuliers). Elle n'est en fait visible par des tiers que dans le cas où d'autres personnes viennent utiliser mon Firefox sur ma machine. C'est le seul cas où on peut avoir envie d'utiliser le mode navigation privée : si on ne souhaite pas qu'une personne utilisant la même machine puisse voir quels sites ont été visités récemment. C'est pourquoi le mode navigation privée est appelé ironiquement « mode pour acheter une bague de fiançailles » [123]. À part ces cas précis, le mode de navigation privée n'apporte que des inconvénients sans apporter d'avantages.

Pour aller plus loin

Paramétrer Ghostery pour éviter les widgets

Les *widgets* sont des « morceaux de sites tiers » qui s'affichent sur le site que vous visitez. Par exemple sur le site d'un journal, on peut trouver des *widgets* Twitter qui affichent des tweets en relation avec l'article lu. On peut aussi trouver un *widget* Facebook pour partager ce contenu avec vos amis ou un *widget* Flickr (le site de partage de photos) où s'affichent des photos publiées sur Flickr par l'auteur de l'article. Le souci avec les *widgets* est que les sites tiers (Twitter, Facebook et Flickr dans nos exemples) sont notifiés de votre visite du site du journal et peuvent ainsi vous pister de site en site.

J'ai pour ma part décidé de bloquer la quasi-totalité des *widgets* avec Ghostery. Il y a toutefois le risque que certains types de contenu, normalement affiché par les *widgets*, n'apparaissent plus, ce qui peut être ennuyeux. C'est pour cette raison que j'ai suggéré de ne pas cocher la case « *Widgets* » dans le paramétrage initial de Ghostery. Mais pour les internautes ayant envie d'être moins pistés, la cocher est une bonne idée, sachant que cela peut être gênant lors de la navigation. Il suffit alors de cliquer sur l'icône Ghostery et réactiver les mouchards et cookies pour le *widget* manquant, pour un site en particulier ou pour tous les sites.

29. Côté messagerie

La messagerie pose de véritables problèmes de fuite des données. En effet, la communication est censée être privée entre les participants, mais les messages transitent en clair sur le réseau, ce qui permet à certains acteurs du numérique de lire le contenu, l'analyser, collecter les listes de vos correspondants de façon à créer un « graphe social » de toutes vos connaissances.

Éviter Gmail

Gmail est l'un de ces acteurs qui utilisent le mail pour enrichir leurs profils, et ils l'affirment haut et fort dans leurs conditions générales d'utilisation :

Nos systèmes automatisés analysent vos contenus (y compris les e-mails) […] lors de l'envoi, de la réception et du stockage des contenus.

Mais au-delà de la lecture de nos emails, Google utilise Gmail comme un cheval de Troie qui permet de suivre un utilisateur dans sa navigation web sur son PC, mais aussi de relier cet utilisateur à son smartphone, lorsqu'il se connecte avec le même identifiant.

Voilà pourquoi se débarrasser de Gmail doit être une priorité pour qui veut limiter le pistage par le géant de Mountain View. Heureusement, quitter Gmail ne signifie pas pour autant abandonner à jamais toute possibilité d'envoyer des emails !

Utiliser une autre boîte aux lettres

La plupart des fournisseurs d'accès à internet proposent des boîtes aux lettres, souvent avec un webmail (possibilité de consulter sa messagerie depuis n'importe quel navigateur web). Il suffit de chercher sur le site de votre fournisseur d'accès comment accéder au webmail et de communiquer à vos correspondants l'adresse qui vous a été attribuée quand vous avez pris votre abonnement à internet. Cette solution vous rend cependant dépendant de ce fournisseur d'accès, votre adresse mail devant changer si vous décidez d'utiliser les services d'un autre. On verra plus loin qu'il est possible de gérer son mail à partir d'un nom de domaine personnel.

Utiliser un client de messagerie

Un client de messagerie comme Mozilla Thunderbird (compatible Mac, Windows et Linux) est téléchargeable gratuitement depuis https://www.mozilla.org/fr/thunderbird/. Comme Firefox, c'est un logiciel libre produit également par la Mozilla Foundation.

Les utilisateurs d'Apple (Mac, iPad et iPhone) peuvent utiliser l'application Mail.app, qui est bien faite, à défaut d'être libre.

Pour les téléphones Android, on pourra utiliser l'application libre K-9 Mail.

Les paramètres nécessaires pour indiquer à ces logiciels quelle boîte aux lettres utiliser sont listés sur le site web de votre fournisseur d'accès. L'usage d'un logiciel de mail rend plus facile le partage de la

lecture du mail sur plusieurs appareils, grâce à l'usage du protocole Imap.

Pour aller plus loin

Rien de ce qui est expliqué ci-dessus n'est très compliqué, mais on peut aller plus loin pour obtenir plus de contrôle sur sa messagerie informatique. Voici quelques pistes à ce sujet.

Encourager ses proches à quitter Gmail

Une fois que l'on a quitté Gmail, Google continue bien souvent à lire nos emails et donc à savoir ce qui nous intéresse. Ce n'est pas de la magie ! Comme Gmail est un grand service de messagerie utilisé par des millions de gens, il y a de fortes chances que parmi nos interlocuteurs, une forte proportion soit encore sous Gmail. De ce fait, Gmail voit transiter nos messages quand nous écrivons à nos contacts qui sont encore sous Gmail. Pour limiter cela, il faut encourager nos proches à quitter Gmail. Cela risque bien sûr de prendre du temps, mais Rome ne s'est pas bâtie en un jour !

Avoir son propre nom de domaine

Cela fait une quinzaine d'années que mon adresse email est tristan@nitot.com, et ça fait toujours son petit effet quand je la communique à un nouveau contact. De plus, cette adresse est facile à mémoriser pour les gens que je rencontre.

Il est tout à fait possible pour tous de disposer de l'équivalent, pour peu qu'on achète son propre nom de domaine, dans mon cas « nitot.com ». Pour cela, il faut aller voir des sociétés comme Gandi.net, Online.net ou OVH.com qui proposent de tels services pour une quinzaine d'euros par an, incluant un nom de domaine (s'il est disponible) ainsi qu'une ou plusieurs boîtes aux lettres, à offrir en cadeau aux membres de la famille !

Apprendre à chiffrer ses messages avec GPG (Gnu Privacy Guard)

Il faut savoir que quand le mail a été inventé, il n'était pas prévu de chiffrer son contenu. Et aujourd'hui, c'est toujours le cas : quand on envoie un email à un correspondant, le message est relayé par plusieurs serveurs de messagerie qui sont susceptibles de le lire. Envoyer un email aujourd'hui, c'est un peu comme envoyer une carte postale sans enveloppe : les postiers peuvent la lire, même si on se doute qu'ils ne le font que très rarement.

Il est possible de chiffrer ses messages, mais cela demande un effort certain. La Free Software Foundation offre un bon tutoriel qui explique bien comment s'y prendre : *Autodéfense courriel* 124.

Il est aussi possible de se rendre dans des événements gratuits appelés « cafés vie privée » 125. Animés par des bénévoles, ce sont des occasions de rencontrer d'autres personnes intéressées par le chiffrement de leurs messages, et d'apprendre le fonctionnement de GPG et d'autres logiciels de chiffrement.

30. Paramétrer Google

Rappelons-le : Google fournit un service gratuit à des utilisateurs en échange de leurs données personnelles, qui sont monétisées auprès d'annonceurs publicitaires. Toutes les actions de Google ou presque participent à l'un de ces deux objectifs : collecter des données sur les utilisateurs ; rendre Google plus utile et donc indispensable à l'utilisateur, via l'utilisation des données collectées.

On a du mal à réaliser à quel point Google collecte des données sur chacun de nous. Sachant que c'est un sujet sensible qui pourrait effrayer de nombreux utilisateurs de ses services, Google liste les données collectées 126, et permet aux utilisateurs d'avoir un aperçu de celles-ci en situation, par exemple notre position au cours du temps, via la page « Vos trajets » (anciennement « Google Location History »), disponible sur https://www.google.com/maps/timeline. On peut voir comment Google, grâce à l'application Google Maps pour smartphone, permet de nous suivre à la trace.

Pour limiter la collecte de données par Google tout en continuant à utiliser certains de ses services, il convient de faire deux choses : demander l'arrêt de la collecte de données futures et supprimer les données déjà collectées de l'historique

Pour cela, nous allons utiliser un service proposé par Google : https://history.google.com/history/.

Passons sur la phrase d'accueil, « *Vous seul pouvez voir ces données* », qui n'est pas tout à fait exacte. En effet, certains employés Google peuvent les voir aussi (voir chapitre 3), mais également certains services de renseignement, soit en ayant fait la demande à Google soit en ayant accédé à votre compte de façon détournée (ce qui doit aussi être le cas de certains tiers mal intentionnés).

La suppression des données est bien cachée dans un menu symbolisé par trois points superposés en haut à droite de la fenêtre. La procédure est la suivante :

Ouvrir le menu en cliquant sur les trois points superposés.

Cliquer sur « Paramètres ».

Dans la fenêtre, repérer l'interrupteur bleu situé à droite de la mention « Votre activité de recherche et de navigation ». Cliquer dessus.

Une demande de confirmation apparaît. Cliquer sur « Désactiver ».

Voilà, c'est fait (au moins pour le stockage futur de vos recherches Google, y compris Google Maps et Google Play Store).

Il nous reste à supprimer l'historique des recherches.

Cliquer sur « Gérer l'historique » pour revenir à la page d'accueil.

Afficher le menu (les trois points superposés) en cliquant dessus.

Choisir l'option « Options de suppression ».

Cliquer sur « Avancé », cocher l'option « Toute la période ».

Cliquer sur « Supprimer » et confirmer votre choix.

Voilà, l'historique de vos recherches a été supprimé.

Il reste encore plusieurs domaines à gérer. Pour chacun d'entre eux, la procédure est la même.

D'abord, passons au domaine suivant. Pour cela, il faut cliquer sur le menu de gauche, symbolisé par trois traits horizontaux superposés (un peu comme un hamburger ou une commode à trois tiroirs).

Pour l'instant, nous sommes encore sur la page « Activité sur le web et les applications », elle apparaît donc en gras et en bleu.

Il faut cliquer sur « Activité vocale et audio » puis reprendre les deux procédures ci-dessus pour d'abord désactiver la collecte des données futures puis supprimer l'historique des données via le menu aux trois points superposés en haut à droite.

Une fois ceci effectué, retourner dans le menu en haut à gauche et sélectionner l'activité suivante, « Informations concernant les appareils » pour refaire la procédure. Faire de même pour toutes les options de ce menu de gauche :

historique des positions ;

historique des vidéos regardées sur YouTube ;

historique des recherches YouTube.

Voilà, en quelques dizaines de minutes pour qui n'a pas l'habitude, nous avons supprimé beaucoup de données sur nos recherches passées et demandé à Google de ne plus stocker nos futures recherches. On notera qu'il est aussi recommandé de se déconnecter de son compte Google après chaque utilisation. Cela peut sembler fastidieux, mais c'est recommandé pour des raisons de sécurité et limite plus encore la quantité de données que Google peut collecter sur nous.

Nous en avons presque fini avec le paramétrage de Google. Il reste encore à empêcher Google de nous pister sur les sites tiers que nous visitons, ce qu'il fait via deux outils : sa régie publicitaire DoubleClick et son système de mesure d'audience Google Analytics.

DoubleClick

DoubleClick est le nom de la régie publicitaire de Google. C'est elle qui affiche des publicités ciblées (donc personnalisées) sur plus de deux millions de sites web dans le monde. Pour cela, elle dispose, sur ces deux millions de sites, de systèmes qui permettent de suivre les internautes en vue d'afficher les publicités ciblées.

Pour éviter ce pistage massif, plusieurs solutions existent. Si vous avez suivi les instructions du chapitre 28 (choisir et personnaliser votre navigateur) et que vous avez installé Firefox avec une extension de type Privacy Badger ou Ghostery, vous n'avez rien d'autre à faire : ces extensions vous protègent du pistage fait par DoubleClick.

Sinon, il est possible d'installer une extension proposée par Google pour empêcher le pistage par DoubleClick (et DoubleClick seulement : elle ne sera pas efficace contre les nombreuses autres régies publicitaires).

Pour cela :

Visiter la page https://www.google.com/settings/u/0/ads/plugin.

Cliquer sur le bouton « Télécharger le plug-in de désactivation du cookie publicitaire ».

Firefox affiche une fenêtre pop-up, cliquer sur « Autoriser » (de façon générale et pour des raisons de sécurité, il est recommandé de ne pas installer d'extensions depuis des sites tiers, mais on fera une exception pour Google).

Firefox affiche le message « N'installer que des modules complémentaires dont les auteurs ont votre confiance ». Cliquer sur « Installer maintenant ».

Redémarrer Firefox.

Notons que cette extension fonctionne aussi sur les navigateurs Google Chrome et Microsoft Internet Explorer, qui ont des systèmes d'extension moins puissants que celui de Firefox.

Google Analytics

Google Analytics est le système de mesure d'audience offert par Google gratuitement à tous les sites qui le souhaitent. Analytics est de loin le numéro un mondial de ce domaine. Il propose aux propriétaires de sites des informations sur les visiteurs de ses pages (Qui sont-ils ? D'où viennent-ils ? Combien de temps restent-ils sur le site ? Quelles sont les pages les plus regardées…).

Plus de 82 % des sites mesurant leur audience ont recours à Google Analytics, ce qui fait que ce dernier peut pister chaque internaute passant d'un site à l'autre.

Il est heureusement possible de ne plus être pisté par Analytics. Comme pour la régie publicitaire DoubleClick, l'utilisation des extensions Ghostery et Privacy Badger ou de bloqueurs de publicité permet d'échapper à la mesure d'audience de Google. Pour ceux qui ne les utilisent pas, Google propose lui-même une extension qui permet de désactiver Analytics. Cette extension fonctionne aussi dans Firefox, Safari, Opera, Chrome et Internet Explorer. Elle peut être installée depuis l'adresse suivante : https://tools.google.com/dlpage/gaoptout

Cliquer sur « Télécharger le module complémentaire de navigateur pour la désactivation de Google Analytics ».

Lire les conditions d'utilisation (c'est recommandé et souvent instructif, mais dans le cas présent assez peu utile).

Cliquer sur « Accepter et installer ».

Firefox affiche une fenêtre pop-up, cliquer sur « Autoriser » (de façon générale et pour des raisons de sécurité, il est recommandé de ne pas installer d'extensions depuis des sites tiers, mais on fera une exception pour Google).

Firefox affiche le message « N'installer que des modules complémentaires dont les auteurs ont votre confiance ». Cliquer sur « Installer maintenant ».

Redémarrer Firefox.

Voilà, nous avons maintenant paramétré Google pour limiter très sensiblement les données qu'il collecte lors de notre utilisation d'internet. Notre quête dans la protection de nos données personnelles peut continuer, cette fois-ci avec notre téléphone mobile…

31. Choisir son smartphone

Les smartphones sont en train de remplacer petit à petit les ordinateurs personnels quand nous utilisons le réseau. Contrairement aux PC, nous les avons toujours avec nous et ils sont connectés en permanence, ce qui les rend d'autant plus précieux et pratiques. Ils sont en plus équipés de tas de capteurs innovants, comme le GPS (qui permet de nous localiser sur la surface du globe), de micros, de caméras, d'un capteur de mouvement (accéléromètre), d'une boussole, etc. Autrement dit, ils sont capables de capter beaucoup plus de données que nos vénérables PC. Et bien évidemment, ces données peuvent intéresser beaucoup de monde. On notera que pour des raisons pratiques, j'englobe ici les tablettes dans le concept de smartphone. Bien souvent, les tablettes utilisent les mêmes systèmes d'exploitation, les mêmes applications et les mêmes composants que les smartphones ; une tablette est essentiellement un smartphone doté d'un grand écran et utilisé sans la puce téléphonique.

Pour ce qui est du contrôle de ces smartphones et des données qu'ils produisent, qui sont nos données, autant le dire tout de suite, j'ai une mauvaise nouvelle : la situation est franchement mauvaise, pour ne pas dire catastrophique.

Afin de mieux comprendre cette situation, faisons le tour du marché, ou du moins des deux principaux acteurs, qui en représentent plus que 95 %.

Android et consorts

Android est le nom du système d'exploitation (le logiciel) qui équipe la grande majorité [127] des smartphones du marché, Samsung en tête, tout comme LG, HTC, Sony et la plupart des fabricants asiatiques. Il y a deux choses intéressantes à propos d'Android. La première, c'est qu'Android est un logiciel en partie libre et en partie propriétaire. Le fait qu'il soit en partie libre pourrait être de bon augure quant au fait qu'on puisse le contrôler (souvenez-vous du chapitre 22 : le fait que le code source soit auditable et modifiable est une condition pour reprendre le contrôle). Pourtant, la partie propriétaire du code gagne du terrain [128] : des portions importantes, auparavant libres, sont remplacées par des équivalents propriétaires et ne bénéficient plus d'améliorations publiques et partagées.

Si Android est gratuit pour les fabricants de smartphones, ceux-ci doivent cependant signer un contrat. Ce contrat, secret, force les fabricants qui veulent diffuser Android sur leurs téléphones à y installer également les applications Google : Maps, Chrome, Search, Gmail, etc. Ces applications, qui capturent nos données et les transmettent à Google sont toutes propriétaires ou sont en train de le devenir. Si Google offre ainsi la possibilité aux fabricants d'utiliser gratuitement le résultat d'investissements de plusieurs centaines de millions de dollars, il attend une chose en retour : la diffusion de ses applications qui lui permettent de collecter nos données et, comme nous l'avons vu au chapitre précédent, de mieux nous connaître, de mieux collecter nos données pour mieux les monétiser et de se rendre toujours plus indispensable.

En substance, Android est un cheval de Troie, un cadeau fait aux fabricants de smartphones pour

qu'ils puissent nous vendre à bas prix des smartphones qui collectent nos données et font de nous de bons utilisateurs de Google afin de nous monétiser auprès des vrais clients de Google, ceux qui payent le géant de Mountain View : les annonceurs publicitaires. Quand je demande à quelqu'un quel téléphone il a, on me répond rarement « c'est un Android », mais souvent « c'est un Samsung » ou « c'est un LG ». Pourtant, peu importe qui fabrique le téléphone, c'est surtout un téléphone dont le logiciel, Android, est fabriqué par Google.

Apple et son iPhone

Apple, deuxième acteur en volume sur le marché des smartphones, a une approche radicalement différente de celle de Google. En effet, Apple conçoit le logiciel et le matériel de ses téléphones, et les vend à un prix haut de gamme, avec des marges très confortables. Même si Apple délègue la production des téléphones à des partenaires, essentiellement chinois, il garde le contrôle sur le logiciel, le design et la distribution. Les marges d'Apple sont si importantes qu'Apple rafle 92 % des bénéfices 129 de toute l'industrie du smartphone alors qu'il représente moins de 20 % des ventes.

C'est plutôt une bonne nouvelle pour notre vie privée : les revenus d'Apple ne viennent pas de l'accumulation de données provenant de ses utilisateurs. Apple, pour faire face à Google, a fait de cet argument son fer de lance, au point de publier sur son site une lettre de Tim Cook 130, son PDG. En voici un extrait :

Il y a quelques années de cela, des utilisateurs d'internet ont commencé à comprendre que quand un service en ligne était gratuit, ils n'étaient pas le client. Ils étaient le produit. Chez Apple, nous pensons qu'il n'est pas nécessaire de sacrifier la confidentialité pour offrir une expérience utilisateur de qualité. Notre modèle d'affaire est très simple : nous vendons d'excellents produits. Nous n'établissons pas de profil en fonction du contenu de vos emails et de vos habitudes de navigation pour le vendre à des publicitaires. Nous ne « monnayons » pas les données que vous stockez sur votre iPhone ou sur iCloud. Et nous ne lisons pas vos emails ni vos messages afin de recueillir des informations pour vous vendre des produits.

Ces propos ont été confirmés dans les faits au printemps 2016, quand Apple a tenu tête au FBI à la suite de l'attentat de San Bernardino, Californie.

Pourtant, il m'est difficile de recommander l'iPhone sans réserves en ayant en tête la volonté de reprendre le contrôle de nos logiciels et de nos données. En effet, de façon générale, et c'est surtout sensible sur l'iPhone plus encore que sur le Mac (l'autre gamme de produits Apple) : Apple est plutôt opposé au logiciel libre et cherche à contrôler tout ce que l'on peut faire avec l'iPhone. L'exemple le plus criant de cette politique est de rendre obligatoire l'usage de l'App Store (magasin d'application d'Apple) pour installer toute application sur son smartphone. Or ce magasin d'applications a des conditions générales d'utilisation qui sont en conflit avec la principale licence de logiciels libres, la GPL 131.

Comme expliqué au chapitre 17, cela pose un double problème :

Il est impossible de faire tourner sur un iPhone un logiciel écrit sous licence GPL, sachant que la GPL est la licence libre la plus utilisée au monde. Dans certains cas, l'ensemble des auteurs du logiciel

peuvent décider d'adopter une autre licence libre telle que la MPL, qui est compatible avec les conditions d'Apple, mais l'obtention de l'accord de tous les développeurs demande énormément de travail non productif.

Apple, en forçant toutes les applications à être installées via l'App Store et en refusant de nombreuses pour des raisons non techniques, joue un rôle de censeur. Bien entendu, la sécurité est souvent utilisée comme prétexte pour protéger une clientèle peu au fait des problèmes de sécurité informatique. Pourtant, c'est souvent une excuse : de nombreuses applications parfois utiles et légitimes ont été refusées au fil des ans, parce qu'Apple ne souhaitait pas associer sa marque à certaines applications.

Aussi, Apple apparaît comme un compromis, où nous sacrifions notre liberté informatique contre un peu plus de sécurité pour nos données personnelles, sans avoir l'assurance qu'Apple ne changera pas de stratégie. Ce compromis évoque la fameuse citation de Benjamin Franklin :

Un peuple prêt à sacrifier un peu de liberté pour un peu de sécurité ne mérite ni l'une ni l'autre, et finit par perdre les deux.

Windows Phone

Au-delà des deux géants du smartphone que sont Google et Apple, d'autres acteurs cherchent à se faire une place au soleil. Microsoft, avec Windows Phone, semble avoir une approche verticale comme Apple, en produisant le logiciel et le matériel (après avoir racheté la marque Nokia), mais sans se concentrer sur le respect de la vie privée, contrairement à Apple. Comme Google, Microsoft semble vouloir tout savoir de l'utilisateur partant du principe que c'est ainsi que le produit sera le plus utile. L'association de son moteur de recherche Bing à un nouveau logiciel de personnalisation appelé Cortana, est décrite de la façon suivante 132 :

Associé à la puissance de Bing, Cortana apprend à tout savoir sur vous et à s'occuper de vous. Cette application va garder un œil sur tout ce qui vous intéresse, vous fera des suggestions utiles, vous rappellera vos réunions et rendez-vous.

Outre le fait que Windows Phone peine à s'imposer malgré les investissements massifs de Microsoft au fil des années dans le mobile, la stratégie utilisée ne semble pas propice à la protection de la vie privée.

Et Firefox OS ?

La fondation Mozilla 133 a lancé le projet Firefox OS durant l'été 2011, en vue de faire un système d'exploitation pour mobile sur la base du navigateur web Firefox. Firefox OS est intéressant pour la reprise de contrôle de l'informatique, dans la mesure où c'est un logiciel libre, donc transparent et auditable, comme tout ce que produit Mozilla. Par ailleurs, la Mozilla Foundation est une organisation à but non lucratif, ce qui la met à l'abri des pressions des actionnaires pour maximiser les profits, même si le financement du logiciel a un coût qu'elle doit nécessairement assumer.

Firefox OS était donc prometteur… jusqu'à ce que la Mozilla Foundation décide d'arrêter d'investir dans Firefox OS pour les smartphones en décembre 2015 et annonce vouloir se concentrer sur les machines connectées, dont les Smart TV. Exit donc Firefox OS, ce qui est d'autant plus dommage que

c'était le meilleur espoir de disposer d'un smartphone grand public faisant tourner du logiciel libre…

Aller plus loin : utiliser Android sans (trop) sacrifier sa vie privée

Tout dans Android est prévu dès le début pour que l'utilisateur stocke ses données chez Google : dès le démarrage, un compte Google / Gmail est demandé. Cela permet ensuite de synchroniser le carnet d'adresses, les mails, l'agenda, le Google Drive de l'utilisateur, tout comme les historiques de navigation, de recherche dans Google Search et Google Maps. Cela est typique de la stratégie de Google qui vise à accéder à toutes nos données pour devenir indispensable à nos vies et à monétiser ces données.

Pas facile, dans de telles conditions, d'utiliser un téléphone Android tout en protégeant nos données. Il reste toutefois plusieurs axes sur lesquels travailler : utiliser des logiciels libres (notamment ceux qui sont proposés sur des dépôts libres) ; utiliser des logiciels proposant du chiffrement ; utiliser des applications se connectant à des services de *cloud* autres que ceux de Google et des grands silos, idéalement des clouds décentralisés (voir chapitre 23) ; utiliser des versions d'Android moins dépendantes de Google.

Utiliser des logiciels libres

Il est possible d'installer des logiciels libres depuis le Google Play Store, mais ce dernier n'indique pas si un logiciel est libre ou non. Comme pour un ordinateur personnel, il est recommandé d'utiliser Firefox à la place de Google Chrome, navigateur par défaut d'Android, pour le respect de la vie privée. Pour cela, procéder ainsi :

Lancer Google Play Store.

Chercher « Firefox pour Android ».

Cliquer sur Installer.

De même, on pourra installer un client de messagerie comme K-9 Mail en remplacement de l'application Gmail, que l'on connectera à son compte mail (idéalement hébergé par un service autre que celui de Google).

Comme il n'est pas évident de repérer les logiciels libres dans Google Play Store, on peut se tourner vers une boutique applicative alternative qui ne recense que des logiciels libres : F-Droid. Voici comment procéder pour l'utiliser :

Visiter le site https://f-droid.org/avec le navigateur web.

Cliquer sur le bouton bleu « Download F-Droid », le téléchargement du fichier FDroid.apk commence.

Une fois le téléchargement terminé (cela peut prendre quelques secondes), lancer l'installation de FDroid.apk.

Il est probable que l'installation soit bloquée pour des raisons de sécurité : Android bloque l'installation d'applications ne provenant pas du Google Play Store. Dans ce cas, nous allons changer le paramètre :

Aller dans les réglages du téléphone.

Choisir l'option sécurité.

Cocher l'option « Sources inconnues » (« Autoriser l'installation d'applications issues de sources inconnues ») et valider ce changement en cliquant sur « OK ».

Revenir au fichier téléchargé et lancer l'installation.

Une fois F-Droid installé, revenir dans les paramètres de sécurité et décocher l'option « Sources inconnues ».

Lancer F-Droid.

Maintenant que F-Droid est utilisable, nous allons le mettre à contribution pour installer de nouveaux logiciels…

Utiliser des logiciels proposant du chiffrement

F-Droid recense plusieurs centaines d'applications libres pour Android, et parmi elles les applications permettant de chiffrer ses communications sont nombreuses.

Le Guardian Project [134] s'est fixé comme objectif de proposer des applications « dans lesquelles on peut avoir confiance », c'est-à-dire qui améliorent la protection de la vie privée, dont la sécurité peut être vérifiée et dont le code est libre.

Chiffrer ses textos

L'application Signal, disponible pour iOS et Android, est gratuite, libre et permet le chiffrement des messages courts de type SMS et MMS. Si le destinataire du message a lui aussi installé Signal, alors les données sont chiffrées, sinon l'application envoie un SMS ou un MMS classique, donc non sécurisé.

Pour aller (encore !) plus loin

Idéalement, pour disposer d'un contrôle maximal sur nos smartphones, il faudrait que la majeure partie du logiciel installé soit libre. Plusieurs communautés de *geeks* se sont attelées à la tâche. En voici quelques-unes :

CyanogenMod : http://www.cyanogenmod.org/ ;

ParanoidAndroid : http://paranoidandroid.co/ ;

OmniRom : http://omnirom.org/ ;

Replicant :http://www.replicant.us/.

Leur installation, qui vise à remplacer la version d'Android installée par le constructeur par une version fournie par la communauté est de plus en plus facile à utiliser, mais elle reste encore hors de portée de la majorité. Aussi, même si j'espère que la pratique visant à installer sur son smartphone un autre système d'exploitation, libre et plus respectueux de la vie privée va se répandre, je constate qu'en attendant, nous sommes réduits à choisir entre différents systèmes, l'un qui capte toutes nos données, et l'autre qui ne nous permet pas d'installer les applications que l'on souhaite.

32. Les médias sociaux

Utiliser les médias sociaux sans pour autant voir ses données personnelles être collectées est un défi, à la limite un défi impossible, du moins avec les médias comme Facebook, dont le patron, Mark Zuckerberg, a déclaré à plusieurs reprises que la vie privée était une chose d'un passé qu'il considérait comme révolu. De fait, Facebook a une politique d'accumulation et de rétention des données particulièrement agressive.

Même les conversations dites « privées » sont en fait susceptibles d'être communiquées par Facebook aux autorités. Le fait divers concernant une jeune allemande refoulée à la frontière américaine 135 nous le rappelle. Elle avait simplement proposé de garder l'enfant de sa cousine habitant les États-Unis (on ignore comment les autorités américaines ont eu accès aux messages. Peut-être tout simplement en regardant dans le smartphone de la jeune femme). Il faut dire que les services américains d'immigration sont particulièrement chatouilleux : ils ont refusé leur entrée sur le territoire à un couple d'Anglais en voyage en Californie 136 car ils avaient publié sur Twitter leur volonté de faire « une fête à tout casser » une fois arrivés.

Voici tout de même quelques conseils pour configurer et utiliser les principaux médias sociaux.

Facebook

Il peut être utile de paramétrer Facebook pour protéger notre intimité numérique vis-à-vis des autres utilisateurs, mais soyons clairs, tout ce que l'on fait sur Facebook est enregistré et bien souvent analysé par le réseau social. Toute tentative pour éviter cela est futile. Il pourrait être tentant d'utiliser un pseudonyme, mais c'est actuellement contraire aux conditions générales d'utilisation de Facebook, qui a déjà supprimé des comptes dans de tels cas. Ceci est susceptible d'évoluer car Facebook semble assouplir sa lutte contre les pseudonymes, mais le risque de perdre nos messages, nos photos et nos interactions n'en vaut probablement pas la chandelle.

Twitter

Twitter semble être beaucoup moins agressif en termes de collecte de données personnelles, c'est pourquoi je suis plus à l'aise à titre personnel avec lui qu'avec Facebook, mais le type d'usage n'est pas le même car il est moins intuitif. Lorsqu'on utilise Twitter, plusieurs paramètres peuvent être modifiés. Pour cela, depuis l'interface web de Twitter :

Une fois connecté, cliquer sur son avatar en haut à droite (par défaut, il représente un œuf).

Cliquer sur « Paramètres ».

Dans la colonne de gauche, cliquer sur « Sécurité et confidentialité ».

Vérifier que la case « Ajouter une localisation à mes Tweets » n'est pas cochée.

Chercher la partie « Contenu sponsorisé » et décocher la case « Personnaliser les publicités en fonction des informations partagées par les partenaires annonceurs. »

Cliquer « Enregistrer les modifications ».

Twitter propose à ses utilisateurs d'honorer le système « Do Not Track », aussi nous allons l'activer. Pour cela, dans Firefox :

Aller dans les préférences.

Sélectionner l'onglet « Vie privée ».

Cocher la case « Pistage / Indiquer aux sites que je ne souhaite pas être pisté ».

Aller plus loin

Pour continuer à utiliser des médias sociaux sans sacrifier sa vie privée, il reste plusieurs approches : chiffrer ses communications au sein du réseau social ; utiliser d'autres médias sociaux plus respectueux de la vie privée.

Datarmine

Datarmine est une initiative intéressante, dans la mesure où elle permet de continuer à utiliser les réseaux sociaux existants, mais en chiffrant le contenu des messages, ce qui rend le contenu lisible uniquement par les destinataires autorisés. Attention toutefois : le réseau social ne peut certes pas lire le contenu du message, mais il connaît ses métadonnées (qui écrit à qui, et quand), ce qui peut en dire presque autant que le message lui-même. Pour essayer Datarmine, visiter le site https://datarmine.com/fr/et installer dans votre navigateur l'extension proposée sur la page d'accueil. C'est elle qui va chiffrer/déchiffrer les messages publiés sur les médias sociaux. Pirouette amusante : sur Facebook, les personnes ne disposant pas de la clé qui permet de déchiffrer le message voient à la place un encart publicitaire pour une association partenaire de Datarmine !

Médias sociaux alternatifs

Il existe plusieurs médias sociaux alternatifs qui sont souvent bien plus respectueux de la vie privée de leurs utilisateurs. J'ai choisi d'en détailler deux : Diaspora* et Movim.

Diaspora* (oui, l'astérisque fait partie du nom !) est un logiciel libre qui fonctionne de façon décentralisée, autrement dit, il est possible de monter son propre serveur faisant tourner Diaspora*, ce qui d'une part permet de choisir un serveur géré par une organisation de confiance et d'autre part évite les problèmes de censure, courants sur Facebook. Par ailleurs, Diaspora* est paramétré par défaut de façon à limiter la dispersion des données personnelles. Par exemple, les métadonnées des photos publiées (comprenant la date, l'heure et parfois la position GPS), sont supprimées avant publication, à moins que l'utilisateur ne spécifie le contraire. Il existe plusieurs centaines de « nœuds » Diaspora* (c'est ainsi qu'on appelle les serveurs de ce média social), à vous de choisir celui dont les conditions générales d'utilisation vous conviennent. Parmi les plus populaires en France, on peut citer Framasphère, opéré par l'association Framasoft, très active dans la lutte contre la centralisation de l'internet avec sa campagne « Dégooglisons Internet » [137].

Movim (qu'on peut utiliser sur http://movim.eu) est lui aussi un média social libre et décentralisé. Il repose de plus sur le protocole standardisé XMPP et les communications sont chiffrées.

Il faut garder à l’esprit que les médias sociaux alternatifs font face à une bataille difficile, et ce pour deux raisons. D’une part, Facebook et les autres médias sociaux ont des moyens financiers qui leur permettent d’investir massivement et de développer sans cesse de nouvelles fonctionnalités pour peaufiner l’expérience utilisateur. D’autre part, il y a un effet réseau dans les médias sociaux : un réseau ne vaut que parce qu’on y trouve des gens à qui on veut parler. Cela favorise les gros réseaux aux dépens des petits et empêche ceux-ci de percer, quand bien même offriraient-ils des avantages inédits comme le respect de la vie privée.

33. Le cloud

À l'heure où nous disposons de plus en plus d'un ordinateur et d'un smartphone, le partage de données entre nos divers appareils est devenu fréquent, ce qui rend nécessaire un système permettant de les synchroniser. Communément appelé *cloud*, l'ensemble de serveurs offrant un tel service est très utile, mais permet trop rarement de préserver la confidentialité des données. Voyons voir comment bénéficier d'un service de *cloud* sans pour autant voir ses données se faire siphonner par un tiers.

On retrouve ici les mêmes limites des modèles commerciaux que dans les chapitres précédents.

Les services commerciaux gratuits, qui comme Google reposent presque tous sur la publicité ciblée, sont incompatibles avec la confidentialité des données dans la mesure où, pour avoir l'air gratuit, il leur faut tout savoir du client, ce qui ne peut être réalisé qu'en accédant à ses données personnelles.

Les services commerciaux *freemium* (deux offres : l'une gratuite et souvent très limitée, l'autre payante avec plus de fonctionnalités) peuvent être une option intéressante dans certains cas. Si les besoins sont limités, on peut parfois se contenter de la version gratuite. Toutefois, il faut garder à l'esprit que le produit est conçu de façon à ce que la version gratuite mette l'eau à la bouche du client mais qu'elle soit suffisamment limitée pour le motiver à passer à la version payante. Pour certaines personnes et certains usages, le *freemium* peut suffire, mais dans biens des cas buter dans les limites (volontaires) du produit peut devenir exaspérant.

On notera que passer au payant contribue à assurer la pérennité du produit (qui veut confier ses données à une société désespérée et prête à tous les compromis pour éviter la faillite ?), mais pas nécessairement la confidentialité des données. En effet, rien n'empêche une société de fournir un service payant tout en profilant ses clients, cumulant ainsi les deux sources de revenus. Pour s'en assurer, il faut lire (et comprendre !) les conditions générales d'utilisation de chaque service, bien souvent écrites dans un jargon juridique ardu, et ce sur des dizaines de pages.

Un service payant hébergé entièrement chiffré

L'inconvénient des systèmes qui stockent nos données chez un hébergeur… c'est que ce dernier y a accès, à moins qu'elles ne soient chiffrées de bout en bout. C'est la notion de *Zero-knowledge* (ne rien savoir) où l'hébergeur ne fait que stocker les données chiffrées qu'il reçoit, sans jamais avoir accès aux données en clair. C'est ce que propose par exemple la société SpiderOak.

Services alternatifs : l'exemple Framasoft

Certains services peuvent être fournis par des organisations dont l'objet est de remplir une mission plutôt que d'enrichir un actionnaire. C'est le cas par exemple de Framasoft, association loi 1901 d'éducation populaire, qui a lancé une campagne intitulée « Degooglisons Internet » https://degooglisons-internet.org/. Framasoft offre gratuitement des services… à condition que les donateurs soient suffisamment nombreux pour assurer le financement des permanents et des coûts associés à ces services.

L’éthique comme valeur première

Framasoft, en prime, a publié une charte de confidentialité 138 qui l’engage dans le respect de la vie privée des utilisateurs de ses services. En voici quelques extraits :

> Liberté du code : Framasoft s’engage à rendre accessible le code source […] Ce faisant, Framasoft démontre sa probité en permettant à chaque utilisateur de vérifier le code source, éventuellement de l’améliorer, et surtout de s’assurer qu’aucun usage déloyal ne sera fait de ses données, de son identité et de ses droits.
>
> Confidentialité : Framasoft s’engage à ne pratiquer aucune censure a priori des contenus, aucune surveillance des actions des utilisateurs, et à ne répondre à aucune demande administrative ou d’autorité sans une requête légale présentée en bonne et due forme. […] Aucune donnée personnelle ne sera exploitée à des fins commerciales, transmise à des tiers ou utilisée à des fins non prévues par la présente charte.
>
> Essaimage : En proposant des applications libres en ligne, Framasoft expose autant d’alternatives aux applications proposées par des entreprises à des fins de monopole et d’usage dévoyé des données personnelles. […] Framasoft s’engage à favoriser leur essaimage en publiant des tutoriels explicatifs sur les méthodes employées pour installer ces applications sur vos propres serveurs.

Des services multiples

Entre 2011 et 2014, 8 services ont été mis en place par Framasoft, qui ont été rejoints en 2015 par 11 autres services. Parmi les plus utiles et donc populaires, on notera :

- Framapad, un bloc-notes collaboratif, alternative très simplifiée à Google Docs ;
- Framadate, un outil pour choisir une date de façon collaborative (alternative à Doodle) ;
- Framacalc, un tableur collaboratif en ligne (alternative à Google Spreadsheet) ;
- Framabag, service de sauvegarde de pages web, alternative à Pocket.

Auto-hébergement

Une approche différente des services en ligne est aussi possible : celle visant à disposer de son service personnel, sur lequel on a tout le contrôle. Cela peut sembler inatteignable au premier abord, mais l’évolution de l’informatique, tant au niveau matériel qu’au niveau logiciel, rend cela bien plus simple qu’on ne pourrait le croire.

De fait, plusieurs solutions techniques sont possibles. Passons-les en revue.

Dispositifs matériels spécialisés à la maison

Avec la baisse de coûts que connaît l’informatique depuis ces dernières décennies, il est possible d’acheter du matériel à un prix raisonnable, avec du logiciel intégré, qui offre des services pouvant remplacer certaines fonctionnalités offertes par des services en ligne. Évidemment, puisque les services sont offerts depuis un système basé à la maison, cela nécessite d’avoir une bonne connexion

internet si l'on souhaite disposer de données lorsqu'on est en déplacement. Pour cela, une connexion ADSL rapide (plus d'un mégabit/s en upload) est nécessaire, et cela sera encore plus efficace si l'on dispose de la fibre (généralement plus de 10 Mbit/s en upload).

Lima

Lima est un petit boîtier qui se connecte d'un côté à son routeur internet (ADSL ou fibre) et de l'autre côté à un disque dur qu'il faut acheter par ailleurs. Une fois les applications installées sur les différents appareils que l'on veut connecter (ordinateur, smartphone, tablette), les fichiers déposés sur l'ordinateur sont accessibles sur les autres appareils (pour l'instant la réciproque n'est pas vraie).

L'attrait de Lima est que pour une somme assez réduite (99 € le boîtier, plus un disque dur à 80 € environ pour un Téraoctet), on dispose d'une solution de partage de fichiers entre appareils qui ne repose pas sur un abonnement. Par ailleurs, les données sont stockées chez soi.

Au-delà des aspects concrets, Lima c'est aussi une étonnante *success story* : les créateurs du produit ont fait une campagne de financement participatif (*crowdfunding*) pour lever 69 000 $ auprès d'internautes. Ils obtiendront 1,2 million de dollars en deux mois, preuve si cela était nécessaire, que la demande pour des produits simples et respectueux de la vie privée est particulièrement forte. À en croire certains articles dans la presse, Lima a encore des progrès à faire avant de devenir un produit parfaitement abouti, mais cela avance.

Les systèmes NAS

Il existe depuis plusieurs années des appareils NAS (*Network Access Storage*), systèmes de sauvegarde sur le réseau local. Ce sont souvent des systèmes RAID, où les données sont stockées sur un groupe de disques durs. Cette logique permet de garantir la pérennité des données même si un des disques tombe en panne. Certains modèles haut de gamme permettent de faire tourner leurs propres applications, comme chez Synology. Un système tel que le Synology DiskStation DS215j (compter 300 € avec les deux disques) permet une sauvegarde des données qui seront accessibles même à distance depuis un smartphone ou un ordinateur portable.

Dans le même genre, en moins puissant, le fabricant de disques durs Western Digital propose MyCloud, pour un peu moins de 200 €.

L'indispensable sauvegarde

À l'occasion d'un incident (vol, incendie, inondation, casse du matériel, etc.), les données peuvent disparaître, d'où l'importance d'avoir un plan de sauvegarde qui met une copie des données à l'abri… dans un endroit distinct. Aussi, une copie de sauvegarde qui serait située dans le même endroit que l'ordinateur ou le NAS n'aura guère d'utilité, car susceptible de subir le même incident au même moment. Il faut envisager une sauvegarde sur un système distant qui ait les mêmes exigences de confidentialité.

Pour aller plus loin : le Cloud personnel

Il existe un certain nombre de solutions qui se conforment plus ou moins au concept de SIRCUS tel que décrit dans la troisième partie de ce livre. Le tableau suivant en présente quelques unes avec leurs spécificités 139.

Nom	Principe	Avantages	Inconvénients	Prix
iCloud	Synchronisation des appareils Apple et accès depuis le web à ces données.	– Interface léchée. – Bonne intégration avec les machines Apple (Mac et iOS). – Modèle payant évitant d'avoir recours à la collecte de données.	– Propriétaire. – Américain (hors de la législation européenne sur la protection des données). – Implique de posséder un appareil Apple (Mac, iPhone ou iPad). Incompatible avec Android, compatibilité limitée avec Windows. – Pas de possibilité de rajouter des applications. – Pas d'auto-hébergement.	Par mois : Gratuit pour 5Go 0,99 € pour 50 Go 2,99 € pour 200 Go 9,99 € pour 1 To.
OwnCloud	Synchronisation de fichiers puis modules tiers.	– Focalisé sur le partage de fichier (façon Dropbox). – Hébergement facile (stack LAMP – Linux, Apache, MySQL, PHP). – Multi-comptes.	– Modèle de sécurité limité entre les comptes d'une même machine.	– Gratuit en auto-hébergement (logiciel libre). – À partir de 2000 € pour 50 utilisateurs.
Sandstorm.io	Déploiement simple d'applications tierces sur un serveur personnel.	– Libre. – Nombreuses applications disponibles.	– Pas de communication entre les applications. – Pas d'intégration. – Nécessite une machine dédiée (ne fonctionne pas avec certains containers).	– Gratuit en auto-hébergement. – Offre commerciale à venir.
Cozy Cloud	– Récupération, gestion et croisement des données personnelles (email, agenda, carnet d'adresses, fichiers, données bancaires, etc.).	– Libre. – Peut être hébergé chez soi ou chez un hébergeur. – Communication entre les applications – Manipulation des données. – Possibilité de récupérer les données d'autres services, dont Google, via des connecteurs.	– Synchronisation de fichiers encore complexe à l'heure où j'écris ces lignes. – Nécessite un hébergeur moderne (acceptant NodeJS et CouchDB) type VPS (serveur dédié virtuel). – Modèle strictement personnel : un seul utilisateur par instance Cozy Cloud.	– Gratuit en auto-hébergement. – Offre commerciale à venir.

Tableau des solutions se rapprochant du concept de SIRCUS.

Notes

113 Pour les premiers, les deux tomes du *Guide d'autodéfense numérique* (accessibles sur https://guide.boum.org/) sont une saine lecture ; pour les derniers, je vous encourage à aller demander de l'aide au commissariat de police le plus proche.

114 On notera le très net recul de Microsoft en termes de respect de la vie privée avec la sortie de Windows 10. La nouvelle version de ce système d'exploitation intègre de nombreux mouchards destinés à pister les utilisateurs. Plusieurs solutions existent pour brider ces mouchards, dont W10Privacy (http://korben.info/windows-10-comment-reprendre-le-dessus.html). Ce domaine évoluant très vite, il est recommandé de se renseigner lorsque l'on se met à utiliser une nouvelle machine sous Windows 10 : de nouveaux utilitaires, plus puissants et plus efficaces ne devraient pas tarder à être publiés pour que chacun puisse disposer d'un Windows 10 respectueux de ses utilisateurs et de leur vie privée. La CNIL s'est émue de cette situation et a produit deux guides pour l'installation et les réglages de Windows 10 – https://www.cnil.fr/fr/reglez-les-parametres-vie-privee-de-windows-10.

115 On se reportera au site http://AV-test.org pour comparer les solutions du moment.

116 https://help.ubuntu.com/community/BackupYourSystem.

117 Pour Opera, c'est particulièrement vrai en ce qui concerne Opera Mini, une version mobile de leur navigateur dont tout le trafic passe par les serveurs d'Opera.

118 Téléchargement d'Adobe Flash Player – https://get.adobe.com/flashplayer/?loc=fr.

119 Téléchargeable depuis https://addons.mozilla.org/fr/firefox/addon/ublock-origin/.

120 Téléchargeable depuis https://addons.mozilla.org/fr/firefox/addon/flashblock/.

121 Mozilla s'y emploie : « Vers l'extinction des plug-ins et la réduction de l'usage de Flash dans Firefox » – *Mozinet*, 21 juillet 2016 – https://blog.mozfr.org/post/2016/07/Reduire-utilisation-Adobe-Flash-Firefox.

122 En fait, mon expérience fait que j'emporte toujours une combinaison de pluie. Toujours. Sinon, il se met forcément à pleuvoir !

123 L'usage de ce mode porte également un nom « que, rigoureusement, ma mère m'a défendu de nommer ici », comme le chantait Georges Brassens.

124 https://emailselfdefense.fsf.org/fr/.

125 éé https://café-vie-privée.fr/ (attention à bien utiliser les accents dans ce cas précis, ce site est l'un des rares qui utilise des accents dans son adresse !).

126 « Quelles sont les données collectées par Google ? » – https://privacy.google.com/data-we-collect.html.

127 80 % en 2015 d'après des statistiques recensées sur Wikipédia – https://en.wikipedia.org/wiki/Mobile_operating_system#Market_share.

128 « Google's iron grip on Android: Controlling open source by any means necessary » (La main de fer de Google sur Android : contrôler le code source par tous les moyens nécessaires), *ArsTechnica*, 21 octobre 2013 – http://arstechnica.com/gadgets/2013/10/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/.

129 « Apple rafle 92 % de la marge du marché des smartphones avec seulement 20 % des ventes », *9to5Mac*, 13 juillet 2015 – http://9to5mac.com/2015/07/13/apple-smartphone-profit-share/.

130 « L'engagement de confidentialité d'Apple », une lettre de Tim Cook – http://www.apple.com/fr/privacy/.

131 « No GPL Apps for Apple's App Store » (Pas d'applications sous licence GPL dans l'App Store d'Apple. VLC, le logiciel qui joue des vidéos vient d'être retiré. Ça ne sera pas le dernier.), *ZDNet*, 8 janvier 2011 – http://www.zdnet.com/article/no-gpl-apps-for-apples-app-store/. On peut toutefois trouver maintenant Firefox sur iPhone, car le projet Mozilla offre Firefox sous trois licences différentes, dont une a pu être acceptée par Apple.

132 « Du PC au smartphone Lumia, Cortana va vous rendre la vie plus facile sur tous vos appareils Windows 10 », *Microsoft* – http://www.microsoft.com/en-us/mobile/experiences/cortana/.

133 Il convient de rappeler que c'est mon ancien employeur, et que cela peut influencer mon analyse, même si je m'efforce à la plus grande objectivité.

134 « The Guardian Project – People, Apps and Code You Can Trust » (Le Gardian Project – des gens, des apps et du code de confiance) – https://guardianproject.info/.

135 « Refoulée des États-Unis à cause d'une conversation sur Facebook », *Rue 89*, 6 août 2015 – http://rue89.nouvelobs.com/2015/08/06/refoulee-etats-unis-a-cause-dune-conversation-facebook-260639.

136 « British tourists' tweets get them denied entry to the U.S. » (Des touristes britaniques se sont vus refuser l'entrée aux États-Unis à cause de leurs tweets), *Time*, 31 janvier 2012 – http://newsfeed.time.com/2012/01/31/british-tourists-tweets-get-them-denied-entry-to-the-u-s/.

137 https://degooglisons-internet.org/.

138 https://n4.framasoft.org/nav/html/charte.html.

139 Remarquons, en toute transparence, qu'à l'heure où j'écris ce livre, je travaille chez Cozy Cloud, une des solutions étudiées.

Et maintenant ?

Les prises de conscience liées à la surveillance de masse sont aussi nombreuses que préoccupantes. Des révélations d'Edward Snowden au débat sur le chiffrement à la suite de l'attentat de San Bernardino, de la loi Renseignement en France à son équivalent russe, nous assistons régulièrement à des événements qui pourraient radicalement modifier notre rapport à nos données personnelles et qui n'ont finalement pas l'impact attendu. Faute d'alternatives, faute de sensibilisation, nous ne modifions pas – ou si peu – nos pratiques quotidiennes, bien que nous en sachions tous chaque jour un peu plus sur la surveillance.

Chacun des acteurs en présence défend sa part du butin. D'un côté, les GAFAM, qui collectent toujours plus de données pour nourrir leur modèle économique, lequel repose sur le profilage de leurs utilisateurs. De l'autre, les États, qui rêvent d'avoir accès à toutes ces données dans une optique de surveillance de masse censée nous prémunir de tous les maux, de la délinquance aux attentats. Comment s'étonner que les premiers multiplient leurs intrusions dans notre intimité par tous les moyens ? Comment s'insurger en voyant que les seconds cherchent à se servir dans les silos à données que sont devenus les data centers ?

Au-delà des critiques sur le bien-fondé d'un tel modèle économique, une question se pose : sommes-nous prêts à laisser des tiers, des acteurs économiques ou des États, tout savoir de nous, quitte à voir nos démocraties muter progressivement vers des États policiers ?

Il n'y a pas de réponse toute faite, et chacun est libre d'arbitrer ce questionnement comme il le souhaite. Avec cet ouvrage, j'espère avoir donné des clefs de compréhension sur les enjeux et mécanismes de la surveillance 2.0, et avoir permis à mes lecteurs et lectrices de mieux cerner le problème. Quant à ceux qui désireraient mieux protéger leur vie privée, j'espère que ce livre leur a apporté des éléments pour agir dès maintenant et retrouver, peu à peu, une forme de souveraineté sur leurs données personnelles.

Paris, le 12 juillet 2016.

Remerciements

De nombreuses personnes ont eu un rôle important dans l'écriture de ce livre, et je redoute l'inévitable perspective d'en oublier. Je prends le risque d'en nommer quelques-unes, au risque de devoir payer un verre à celles et ceux que j'oublierais.

Pour commencer, ceux qui m'ont décomplexé au tout début du projet au point que je me suis autorisé à me lancer : Camille Gévaudan et Erwan Cario, mes complices de l'émission *56Kast* (NoLife / Libération). Immédiatement après, Muriel Shan-Sei-Fan et Thierry Noisette, qui m'ont rassuré sur la faisabilité du projet.

Mes employeurs, Mozilla et Cozy Cloud, pour avoir soutenu ce projet qui m'a occupé plus que je ne l'imaginais à l'époque.

Ensuite, les lecteurs du *Standblog* qui ont fait office de relecteurs et surtout sources de motivation pour continuer la rédaction, grâce à la publication par épisodes. Parmi eux, plusieurs ont été source d'inspiration : Goofy, Jef Mathiot, Olivier Olicat, Jb Piacentino, Marie-Odile, V_atekor, Pierre Lotigie-Laurent.

Des experts dont Claire Levallois-Barthe sur les aspects juridiques de la vie privée et les hackers (au sens le plus noble du terme) : Ens0, Okhin, Genma, Axx, Taziden sur les aspects technique et sécurité ; Pierre-Luc Paour et Olivier Meunier pour le mobile. Comme le dit la formule consacrée : le savoir vient d'eux, les erreurs viennent de moi.

Mes éditeurs, Hervé Le Crosnier et Nicolas Taffin de C&F éditions, qui m'ont redonné foi en l'édition, ce qui n'est pas peu dire.

Mention spéciale à Nina Cercy de Cozy Cloud, pour l'élan dans la toute dernière ligne droite !

Les projets de La Quadrature du Net et de Café Vie Privée, qui font un indispensable travail d'éducation populaire avec un impact bien plus important que leurs moyens ne leur permettent.

Enfin, mon épouse Bénédicte qui, avec les longues heures de travail, a tendance à trouver que son mari se disant féministe joint trop rarement le geste à la parole. Et bien sûr mes enfants, Robin et Philippine, qui forcent la fierté de leurs parents et que les absences trop fréquentes de leur papa n'empêchent pas de s'épanouir.

Et puis bien sûr vous, lecteurs et lectrices, que je remercie d'avoir eu le courage de vous documenter sur ce sujet important, et pour votre ténacité afin d'arriver à cette toute dernière ligne !

C&F éditions

Crée en 2003 et animée par Nicolas Taffin et Hervé Le Crosnier, C&F éditions propose des ouvrages imprimés, numériques, et des sites multimédias.

Renseignements, contacts, publications et services : http://cfeditions.com

Derniers titres parus

C'est compliqué : Les vies sociales des adolescents connectés, danah boyd (traduction par Hervé Le Crosnier), Collection *Les enfants du numérique*, juin 2016, 432 p.

La tête dans la toile, Xavier de la Porte, Collection *Blogollection*, mars 2016, 508 p.

En communs : une introduction aux communs de la connaissance, Hervé Le Crosnier, Collection *Blogollection*, octobre 2015, 254 p.

Grandir connectés : les adolescents et la recherche d'information, Anne Cordier, Collection *Les enfants du numérique*, octobre 2015, 304 p.

Pages publiques : à la recherche des trésors du domaine public, ouvrage coordonné par Nicolas Taffin, juin 2014, 128 p.

Le souffle de la liberté : 1944, le jazz débarque, Nicolas Beniès. Ouvrage accompagné d'un CD audio, mai 2014, 158 p.

Culturenum : jeunesse, culture & éducation dans la vague numérique, ouvrage coordonné par Hervé Le Crosnier, septembre 2013, 207 p.

Aux sources de l'utopie numérique : de la contre-culture à la cyberculture, Stewart Brand un homme d'influence, par Fred Turner (traduction Laurent Vannini), décembre 2012, 428 p.

Dans le labyrinthe : évaluer l'information sur internet, Alexandre Serres, juin 2012, 224 p.

Licence Édition Équitable

La lecture n’est pas réductible à une consommation. C’est une activité productive et sociale, et non passive et solitaire. La licence Édition Équitable vise à promouvoir les droits des lecteurs et lectrices. Elle présente également le rôle de l’éditeur, proposant entre lecteur et éditeur un contrat équitable et durable.

Un livre (ou autre support culturel) est le produit d’une collaboration entre les auteurs, responsables de l’œuvre, et l’éditeur qui porte ce travail jusqu’au public. Les métiers de l’édition ne disparaissent pas avec l’internet, ils se renouvellent. Les auteurs, les musiciens, les graphistes,... peuvent toucher directement un large public grâce à l’internet. Les éditeurs (ou les producteurs des autres supports) restent néanmoins indispensables pour la sélection, l’établissement, la traduction, la relecture, la composition typographique, la présentation et l’accompagnement de l’auteur. Leur métier consiste à transformer les créations en documents édités...

Les auteurs disposent des Licences Creative Commons pour indiquer au lecteur ce qu’il peut faire avec leur œuvre. La Licence Édition Équitable vise à remplir le même rôle pour définir les droits du lecteur et ses responsabilités envers le processus éditorial. Un document édité sous la Licence Édition Équitable assure aux lecteurs les libertés et droits inaliénables suivants :.

> Le lecteur/lectrice a le droit de lire (écouter, visionner pour les multimédias) le document sur les appareils de son choix et sur la durée la plus longue possible. Ceci exclut l’usage de verrous numériques ou autres méthodes de cryptage.
>
> Le lecteur/lectrice a le droit de copier le contenu sur les supports privés dont il dispose, de changer les formats au besoin, pour ses usages personnels et dans son cercle de proximité.
>
> Le lecteur/lectrice a droit de copier des extraits dans ses propres documents (textes, rapports, analyses, blogs, articles,...) sous réserve de mentionner l’édition originale de l’œuvre et les informations nécessaires au respect envers les auteurs (citation et le cas échéant lien vers les sites de l’auteur ou du document).
>
> Le lecteur/lectrice a le droit de rediffuser le contenu de l’œuvre en respectant les volontés de l’auteur quand elles sont exprimées par une licence d’usage. Ceci est distinct de la rediffusion du document édité (livre, notamment livre numérique, album musical, et cela plus encore s’il s’agit d’œuvres de collaboration ou de compilation).
>
> Le lecteur/lectrice a le droit de faire circuler le document édité au sein de son cercle de proximité (y compris élargi à ses amis proches). Toutefois, cette liberté ne permet pas de rompre l’équilibre et l’équité en diffusant massivement ou à des inconnus.

Pour l’application de ces droits, le lecteur s’engage à respecter le travail éditorial, en citant à chaque fois que c’est possible, la source éditoriale permettant à une autre personne d’acquérir le document édité : site web de l’éditeur, site spécifique d’un livre ou d’un album musical, plate-forme de vente...

Version de référence : http://edition-equitable.org

Achevé d'imprimer

C&F éditions tient à remercier Antoine Fauchié (http://quaternum.net) pour la réalisation de cette version numérique.

Ce livre numérique est publié en octobre 2016 par C&F éditions.

Il est diffusé sous licence Édition Équitable (http://edition-equitable.org).

Le corps du texte est en police Libertine (http://www.linuxlibertine.org/), une police libre diffusée sous licence SIL-Open Font Licence (http://scripts.sil.org/cms/scripts/page.php?item_id=OFL).

Les titres et intertitres et les notes de contexte sont en police Sinkin Sans (http://www.k-type.com/fonts/sinkin-sans/), produite par K-type et diffusée sous licence Apache.

Achevé d’imprimer en septembre 2016.
Dépôt légal 3e trimestre 2016.
Version imprimée : ISBN 978-2-915825-65-7
Version numérique : ISBN 978-2-915825-66-4
Bundle (imprimé + numérique) : ISBN 978-2-915825-67-1
http://cfeditions.com

- Couverture
- Page de titre
- Table des matières
- Préface par Adrienne Charmet
- Avant-propos
- Première partie
- Souriez, vous êtes surveillés !
  - 1. Est-il si grave de perdre le contrôle de son ordinateur et de son smartphone ?
  - 2. Les risques personnels
  - 3. Google sait tout sur nous, voici comment
  - 4. Facebook, la manipulation des masses et la démocratie
  - 5. La surveillance des États
  - 6. Big Data et grosses responsabilités
  - 7. L’impact de la surveillance sur la société
  - 8. Loi et vie privée
  - 9. Mais, je n’ai rien à cacher !
- Deuxième partie
- Au royaume d’internet, le code, c’est la loi
  - 10. Contrôler pour ne pas être contrôlé
  - 11. Que peut-on contrôler ?
  - 12. Contrôle et informatique personnelle
  - 13. Le code, c’est la loi
  - 14. Internet change la donne
  - 15. Le piège de la gratuité
  - 16. Le modèle freemium
  - 17. Faut-il avoir confiance en Apple ?
  - 18. Smartphones et Cloud
  - 19. Internet des objets, quantified self et beacons
  - 20. Les services de renseignement
- Troisième partie
- Un autre réseau est possible
  - 21. Sept principes pour reprendre le contrôle
  - 22. Le logiciel libre
  - 23. La maîtrise du serveur
  - 24. Le recours au chiffrement
  - 25. Penser le modèle d’affaire
  - 26. Faire mieux que les systèmes centralisés
- Quatrième partie
- Un internaute averti en vaut dix
  - 27. Partir sur de bonnes bases
  - 28. Choisir et personnaliser son navigateur
  - 29. Côté messagerie
  - 30. Paramétrer Google
  - 31. Choisir son smartphone
  - 32. Les médias sociaux
  - 33. Le cloud

- Et maintenant ?
- Remerciements
- À propos de C éditions
- Licence dition quitable
- Achevé d'imprimer